

UNIVERZITA KARLOVA

Právnická fakulta

Marek Poloni

Regulace internetu

Diplomová práce

Vedúci diplomovej práce: Prof. JUDr. Richard Pomahač, CSc.

Katedra: Správni právo

Dátum vypracovania práce (uzatvorenie rukopisu) : 18.4.2018

Prehlasujem, že som predkladanú diplomovú prácu vypracoval samostatne, že všetky použité zdroje boli riadne uvedené a že práca nebola využitá k získaniu iného alebo rovnakého titulu.

Ďalej prehlasujem, že vlastný text práce vrátane poznámok pod čiarou má 256.414 znakov, a to vrátane medzier.

Marek Poloni
diplomant

V Prahe dňa 18. apríla 2018

OBSAH

ZOZNAM POUŽITÝCH SKRATIEK:	5
ÚVOD	6
1 HISTORICKY A PRÁVNE O REÁLIÁCH INTERNETU	10
1.1 „TAXONÓMIA“ INTERNETU	12
1.1.1 <i>Na obranu kyberpráva</i>	15
1.2 UMENIE (VRCHNOSTENSKEJ) REGULÁCIE	18
1.2.1 <i>Konštrukčné atribúty regulácie</i>	21
1.3 KONTEXT HISTÓRIE INTERNETU	24
1.3.1 <i>Počiatky Internetu</i>	24
1.3.2 <i>Podiel súkromných subjektov na vývoji modernej internetovej siete</i>	27
2 TEÓRIA REGULÁCIE KYBERPRIESTORU	30
2.1 OBECNÉ ÚVAHY O INTERNETE, KYBERPRIESTORE A NUTNOSTI JEHO REGULÁCIE	30
2.1.1 <i>Príbeh o dvoch kyber_mestách</i>	32
2.2 LEGITIMITA A EFEKTIVITA KÓDU A NORIEM V KYBERPRIESTORE	34
2.2.1 <i>Definičné authority</i>	37
2.3 INTERNETOVÝ GATEKEEPING	38
2.3.1 <i>Rámec Network Gatekeeper Theory</i>	40
2.3.2 <i>Voľne k problémom internetovej regulácie</i>	44
3 PRÁVNA ZODPOVEDNOSŤ PRI POUŽÍVANÍ INTERNETU	46
3.1 DOKTRINÁLNE VÝCHODISKÁ POSKYTOVANIA SLUŽIEB INFORMAČNEJ SPOLOČNOSTI	48
3.2 KRÁTKO KU ROZDIELU PRENOSU A ŠÍRENIA OBSAHU	50
3.2.1 <i>Informačná spoločnosť</i>	52
3.2.2 <i>Služba informačnej spoločnosti</i>	53
3.2.3 <i>Poskytovateľ služieb informačnej spoločnosti</i>	58
3.2.4 <i>Užívateľ služby informačnej spoločnosti</i>	59
3.3 PRÁVNÝ KONCEPT ZODPOVEDNOSTI V PROSTREDÍ INTERNETU PODĽA ZÁKONA Č. 480/2004 SB.	60
3.4 VYLÚČENIE Z REŽIMU VŠEOBECNEJ ZODPOVEDNOSTI	63
3.4.2 <i>Mere conduit</i>	67
4 PRÍSTUP K OTVORENÉMU INTERNETU A BLOKOVANIE PRÍSTUPU K OBSAHU	71

4.1	PRÍSTUP K PROBLEMATIKE OTVORENÉHO INTERNETU V EURÓPSKEJ ÚNII	73
4.1.1	<i>Zabezpečenie prístupu k otvorenému internetu</i>	76
4.2	ZÁKLADNÉ POSTOJE K BLOKOVANIU PRÍSTUPU K OBSAHU	81
4.2.1	<i>Model krajín s nedostatočným národným regulačným rámcom</i>	83
4.2.2	<i>Model krajín s cieleným národným regulačným rámcom</i>	84
4.3	PRÁVNE VÝCHODISKÁ V ČESKEJ REPUBLIKE	86
4.4	VYBRANÉ PROBLÉMY TRESTNOPRÁVNEHO RÁMCA	89
4.4.1	<i>Spoločný boj proti sexuálnemu zneužívaniu detí na internete</i>	93
4.5	VYBRANÉ PROBLÉMY SPRÁVNOPRÁVNEHO RÁMCA	96
4.5.1	<i>Možnosti regulácie nelegálneho hazardného hrania na internete</i>	99
4.5.2	<i>Rozbor ustanovení o blokácii nepovolených internetových hier</i>	105
	ZÁVER	112
	ZOZNAM POUŽITÝCH ZDROJOV	120

Zoznam použitých skratiek:

ISP	Poskytovateľ služieb informačnej spoločnosti
MFČR	Ministerstvo Financí Českej republiky
smernica o e-obchode	Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode)
SŘ	Zákon č. 500/2004 Sb., správní řád,
SŘS	Zákon č. 150/2002 Sb., soudní řád správní
TZ	Zákon č. 40/2009 Sb., trestný zákoník
TŘ	Zákon č. 141/1961 Sb. trestní řád
ZoHH	Zákon č. 186/2016 Sb., o hazardních hrách
ZoElKom	Zákon č. 127/2005 Sb., o elektronických komunikacích
ZoNSIS	Zákon č. 480/2004 Sb. o některých službách informační společnosti a o změně některých zákonů

Zákony v znení neskorších predpisov v stave ku dňu 26.3.2018

„SOKRATES: Alebo znova, na lodi, ak má človek právomoc robiť tak ako si zmyslí, ale postretá inteligenciu a zručnosť v navigácii [*αρετης κυβερνητικης, aretes kybernetikes*],
vidíš, čo sa stane s ním a jeho námorníkmi?
ALCIBIADES: Áno; Vidím, že všetci zahynú! “

Úvod

Táto diplomová práca sa skladá z troch hlavných tematických okruhov. V prvej časti s názvom „Historicky a právne o reáliach internetu“ sa venujeme najmä významu pojmu Internet, s ohľadom na poňatie informácie ako organizačného inštrumentu v kybernetike. Predostrieme základné súvislosti významu vývoja samostatného právneho odvetvia vo svetle prístupu k právnemu zakotveniu regulácie. Pokúsime sa zachytiť nielen technologicko-historický vývoj internetu, ale rovnako aj pramene myšlienkového progresu jadra regulácie, a to v kontexte súčasného celospoločenského dopadu. V druhej časti tohto celku s názvom „Teória regulácie kyberpriestoru“ stanovíme hranice konceptu kyberpriestoru², ktorú budeme doprevádzať polemikou nad nutnosťou a primeranosťou rôznych prostriedkov jeho efektívnej regulácie a otázkou, kto a akými prostriedkami kyberpriestor skutočne reguluje. Našou úlohou bude aplikovať všeobecné abstraktné koncepty a pojmy na prostredie kyberpriestoru. Taktiež voľne nastienime základné právne problémy vznikajúce v prostredí Internetu a výsekový rámec modernej ochrany určitých základných ľudských práv pomocou tzv. *gatekeepingu*.

Na filozoficko - teoretickú úvahu bližšie nadviažeme druhým tematickým okruhom, výkladom právnej úpravy zodpovednosti niektorých poskytovateľov služieb informačnej spoločnosti na českej a európskej úrovni. V tretej časti užšie vymedzíme právnu reguláciu

¹ PLATÓN. *Alcibiades I.* preklad JOWETT, Benjamin [online]. Publikované 21.2.2008 [cit. 31.3.2018]. Dostupné z: <http://www.gutenberg.org/files/1676/1676-h/1676-h.htm>. slovenský preklad autora.

² Abstraktný filozofický koncept: „Konsenzuálna halucinácia denne prežívaná miliardami legitímnych operátorov v každom národe deťmi, ktoré sú vyučovaní matematické koncepty (...). Grafické znázornenie údajov odobratých z databáze každého počítača v ľudskom systéme. Neodmysliteľná zložitosť. Riadky svetla sa nachádzali v bezpriestore mysle, zhlukov a súhvezdí údajov. Rovnako ako mestské svetlá, ktoré ustupujú.“

Citácia: GIBSON, William. *Neuromancer*. New York: Ace Books, 1984, 288 s. ISBN 9780441569595. s.51

zodpovednosti za šírenie a zverejňovanie informácií prostredníctvom Internetu jeho užívateľmi s prihliadnutím k zneniu ZoNSIS a ZoElKom.

V nadväznosti na tému zodpovednosti budeme pokračovať výkladom posledného tematického okruhu v štvrtej časti - súčasnej problematike zabezpečenie otvoreného prístupu k internetu a jeho obsahu a možnostiam blokovania prístupu k určitému zverejnenému obsahu. Stanovíme si modelové systémy právnej úpravy blokovania stránok s určitým obsahom a rôznych prístupov súkromných subjektov a štátu. Bližšie budeme skúmať právny rámec v Českej republike, hlavne vo vybraných oblastiach trestného a správneho práva.

V diplomovej práci podporíme vyššie uvedené kontextuálne úvahy hlavne teleologickým výkladom pozitívneho práva v tretej a štvrtej časti. Neustálená doktrína nového právneho odvetvia a regulácie poskytuje priestor subjektom k aktívnej participácii na jej vývoji. Predpokladom je však zvolenie vhodnej definície jej presných špecifik a súčasne zohľadniť vecné otázky ako efektívnosť a legitimita práva, ako i nevýhody prameniace z neistoty aplikácie z analogickej interpretácie.

Snahou tejto diplomovej práce nie je poukázať na faktickú správnosť názorov zástancov deregulácie, autoregulácie ani výlučne štátnej regulácie internetu, ale naopak priblížiť pohľad všetkých zúčastnených subjektov a zachytiť rozmanitosť a zložitnosť vznikajúcich právnych vzťahov za súčasného priblíženia previazanosti verejného a súkromného práva v tomto prostredí. Práve z uvedených dôvodov som si ako cieľ práce určil popísanie vybraných aspektov v čase sa rozvíjajúceho právneho odvetvia nielen v kontexte rigidného právneho uvažovania, ale i s prihliadnutím k logickej štruktúre protikladných názorových škôl. V prípade, že predpokladom je dopracovanie sa analytickým výkladom k súhrnnej premise odôvodnenej nutnosti prostredie internetu právne regulovať, za základné otázky, na ktoré budeme v priebehu práce hľadať odpovede sú nasledujúce:

- a) Do akej miery je prostredie internetu nutné právne regulovať ?

- b) Je oprávneným verejným záujmom oslobodiť tieto nové a poučné služby z pút storočnej rigidnej regulácie?³
- c) Akým smerom by sa mala uberať legislatívna tvorba v odboroch regulácie práv a zodpovednosti na internete a prístupe ku komunikačnej sieti?

Pri písaní tejto práce si sľubujem rozšírenie ohraničených kontúr teoretickým výskumom tejto perspektívnej a dynamicky sa rozvíjajúcej právnej disciplíny, ku ktorej v súčasnej dobe neexistuje nutne jednotný ani ucelený názor. Zároveň verím, že pri písaní tejto diplomovej práce získam cenné podklady pre profesionálne smerovanie v poznaní a formovaní tejto právnej disciplíny.

Mladosť tohto odboru v českom prostredí so sebou prináša i veľkú absenciu literatúry k danej problematike, obzvlášť v slovenskom a českom jazyku. Z týchto dôvodov a vzhľadom k primeranosti substrátu tejto diplomovej práce si dovoľím čerpať predovšetkým zo zahraničnej literatúry ako i zdrojov dostupných online, či už sa jednalo o odborné články, univerzitné zverejnené výskumy či blogové príspevky právnikov a zainteresovanej verejnosti. Pre doplnenie uvádzam, že väčšina použitých materiálov je dostupná len v anglickom jazyku. V takomto prípade som pre citáciu použil vlastný primeraný slovenský ekvivalent na základe vlastného prekladu. V prípade nenájdenia vhodného ekvivalentu som výraz ponechal v pôvodnom znení.

Sémantickým problémom tejto práce je i odlíšenie Internetu ako vlastného mena objektu, ktorý je súhrnom všetkých služieb v celosvetovej informačnej a komunikačnej sieti a internetu ako spôsobu komunikácie fyzickým prepojením sietí spoločným protokolom⁴. Savický, pragmaticky navrhuje všeobecné použitie malého „i“ nakoľko sa pôvodný zmysel technického pojmu Internet vytráca a stáva nepraktickým. Použiť by sme ho mohli napríklad v kontexte historického vývoja celosvetovej siete, ako hovorí Peterka: „*Internet s veľkým I je*

³ Otázku je prebratá od komisára Roberta McDowell z Institute for Policy Innovation (IPI) z diskusie o Internetovej regulácii z dňa 12.11.2009. [cit. 14.2.2017]. Dostupné z: https://apps.fcc.gov/edocs_public/attachmatch/DOC-294631A1.pdf

⁴ SAVICKÝ Jan, *Internet se bude psát s malým i* [online]. Príloha internetového denníku Neviditelný pes v týždni od 22. septembra do 29. septembra 1997 [cit. 27.3.2018]. Dostupné z webového archívu: web.archive.org/web/20020903231020/http://pes.eunet.cz:80/97/39/0039ar08.htm

*len jeden, internetov s malým i sú tisíce*⁵. V českých i zahraničných médiách sa čoraz viac zaužívalo druhové obecné označenie „internet“⁶, s ktorým budeme prevažne pracovať i v tejto práci, zatiaľ čo na pojem „Internet“ adekvátne odkážeme v historicko - filozofickom zmysle ako ideálu celosvetovej komunikačnej siete.

Táto diplomová práca reflektuje stav právnej úpravy a názorové východiská odbornej verejnosti ku dňu 18. 4. 2018.

⁵ Citát Jiřího Peterky z 29.9.1997 prevzatý zo stránky webhouse.cz/versus/ii/. Jednalo sa o *Volné sdružení za psání slova internet s malým písmenem i, aneb Internet versus internet*, s možnosťou užívateľského hlasovania, pri ktorom prevládalo písanie slova Internet [cit. 27.3.2018]. Dostupné z webového archívu na:

<http://web.archive.org/web/20030704002338/www.webhouse.cz/versus/ii/>

⁶ Viac k hnutiu českému i zahraničnému prechodu na pojem *internet* ako pojmového druhového mena ZEMAN Mirek, *Internet vs. internet* [online]. Lupa.cz, publikované 30.8.2004 [cit. 27.3.2018]. Dostupné z: www.lupa.cz/clanky/internet-vs-internet/ alebo SCHWARTZ John, *The Nation: Case-Sensitive Crusader; Who Owns the Internet? You and i Do* [online]. The New York Times, publikované 29.12.2002 [cit. 27.3.2018]. Dostupné z: www.nytimes.com/2002/12/29/weekinreview/the-nation-case-sensitive-crusader-who-owns-the-internet-you-and-i-do.html

1 Historicky a právne o reáliách Internetu

V prvej kapitole prihliadneme k technologickému substrátu, organizačnej štruktúre a ideám, ktoré viedli k vzniku Internetu a jeho modernej regulácie. Ako základné východisko si priblížime axiómu Internetu ako ohraničenie virtuálneho priestoru – kyberpriestoru. Ten je z normatívneho hľadiska zvláštnym objektom *sui generis* a čiastočne nás núti opustiť medze kritickej jurisprudencie a rigidného legalizmu v prospech interdisciplinárneho prístupu nie nepodobnému technokracii⁷. Ak by hypotézou bol predpoklad obsiahnutia definičnej podstaty internetu tradičnými právnymi metódami, dispozíciou by zaiste bolo oprávnenie tento objekt celistvo autoritatívne regulovať. To však, ako predstavíme v tejto práci, nie je objektívne možné. Regulácia internetu podlieha podobnej právne technickej decentralizácii ako aj jej samotný objekt či právna disciplína, ktorá sa ním normatívne zaoberá. Preto si ako predmet výkladu prvých dvoch častí stanovíme i zamyslenie o predmetných východiskách rezignácie na tradičné pozitívnoprávne myslenie a legitímite metód uplatňovania práva na vzťahy v kyberpriestore.

Prvotne si však pripomeňme Sokratove slová z úvodu práce, ktoré pojednávajú o potrebe osvojenia si umenia riadiť plavidlo ako predpoklad kontroly od proverbiálneho chaosu. Z derivátu gréckeho slova zaoberajúceho sa štúdiom o samo-riadení vzniká jednostranný pojem "kybernetika" predstavujúci široký pojem zahŕňajúc všetky procesy v systéme riadenia, komunikácie a spätnej väzby a poznanie ich všeobecných zásad⁸. Johnson tento pojem etymologicky zjednocuje i s umením regulácie v zmysle „*governance*“⁹. V našom prípade kapitánom lode zdatným v riadení je regulátor vedúci pomyselnú metaforu

⁷ Inšpirované abstraktom DOUZINAS, Costas a GEAREY, Adam. *Critical jurisprudence: the political philosophy of justice*. Oxford, UK: Hart Publishing, 2005, 370 s. ISBN 184113452X

⁸ PIOTROWSKY, Robert. Between Plato and Wiener. Philosophical cybernetics in the 17th century. *Studies in Logic, Grammar and Rhetoric*. Roč. 2012, č. 28(41), s.63-71. ISSN 2450-6842

⁹ Srov. s teleologickým výkladom pojmov. JOHNSON, Barnabas D. *Cybernetics of Society. The Governance of Self and Civilization* [online]. Jurlandia.org [cit 31.3.2018] Dostupné z: www.jurlandia.org/cybsoc.htm#Conclusion

lode štátu¹⁰. Kybernetiku ďalej v modernom poňatí rozvinul Weiner vo svojej knihe rovnakého titulu ako štúdium kontroly a komunikácie so zvieratom a strojom, čím prvýkrát spojil kontrolu ako retroaktívnu činnosť vykonávanú za účelom dosiahnutia cieľov s komunikáciou ako spojenie a tok informácií medzi aktérom a prostredím¹¹. Inými slovami, pozoroval kruhový príčinný vzťah v systéme, kde akákoľvek činnosť systému spôsobuje určitú zmenu prostredia a táto zmena je prezentovaná systému v podobe informácie alebo spätnej väzby, ktorá mení spôsob správania sa systému v záujme dosiahnutia jeho cieľa¹². Tento mechanizmus kontroly a komunikácie môžeme uplatniť nielen vo fyzickom, či organickom prostredí, ale taktiež v sociálnych štruktúrach a odvodených koncepciách ako organizácia či samoorganizácia prostredia. Wiener v tomto zmysle jednoducho poukazuje na to, že efektívna akcia si vyžaduje komunikáciu. Je zrejmé, že dôležitosť informácie a komunikácie ako mechanizmov organizácie prebieha nad rámec jednotlivca a do vnútra spoločenstva¹³. Poukazuje na to, že týmto spôsobom organizmy a prenesene i systémy čelia entropii¹⁴, ktorej prirodzenou tendenciou je rásť. Tým sa akýkoľvek systém zhoršuje a stráca

¹⁰ LUCA, Dumitru, SIRGHI Lucel, COSTIN Claudiu. *Recent Advances in Technology Research and Education*. Springer International Publishing, 2018. ISBN 9783319674589. s.336

¹¹ WIENER, Norbert. *Cybernetics, Second Edition: or the Control and Communication in the Animal and the Machine*, vyd. 2. The MIT Press, 1965, 212 s. ISBN 026273009X

PANGARO, Paul. *Cybernetics - a definition* [online]. Pangaro, 1990. [cit. 4.4.2018]. Dostupné z: pangaro.com/definition-cybernetics.html

¹² ADAME, Talia. *Handbook of Cybernetics* [online]. Rev. Vyd. 2016. New York: Library Press, 2016, 90s. ISBN 9781280298202. s.5 a násl. [cit. 4.4.2018]. Dostupné z WTbooks: ebooks.wtbooks.com/static/wtbooks/ebooks/9781280298202/9781280298202.pdf

¹³ WEINER, Norbert, op. cit. *Cybernetics*, 1965. s. 18 a násl.

¹⁴ Pojem *entropia* má viacero významov podľa disciplíny, ktorá s pojmom pracuje. V zásade aplikujeme na sociálne prostredie druhý zákon termodynamiky, ale pre potreby práce poukazujeme na entropiu taktiež v zmysle teórie informácie a štatistiky rozvinutej napr. matematikmi J. Willard Gibbs a Claude Shannon. Pojem používame ako mieru neusporiadanosti či náhodnosti v rámci uzavretého systému a ako nevyhnutnú deterioráciu systému či spoločnosti. Srov. napr. BARTÁK, Matěj, VEBROVÁ, Jitka a RYCHLÁ, Renata ed. *Nový slovník cizích slov pro 21. století*. Praha: Plot, 2008, 367 s. ISBN 9788086523897. s. 94, alebo zdroje dostupné online: slovník-cizich-slov.abz.cz/web.php/slovo/entropie

sebarozlišovaciu spôsobilosť, čím prechádza zo stavu organizovanosti a odlíšenia do stavu rovnakosti a chaosu¹⁵. Poznamenáva, „rovnaako ako entropia je mierou dezorganizácie, informácie prenášané súborom správ [komunikáciou] je mierou organizácie¹⁶“. Prečo je však tento poznatok pre nás dôležitý?

Vyššie sme uviedli, že úlohou tejto práce nie je ozrejmovat' technickú podstatu internetových sietí, ale rozvinutie chápania Internetu ako decentralizovaného sociálneho systému, do ktorého vstupujú subjekty s rôznou úrovňou authority. K pochopeniu kybernetického princípu riadenia procesov v prostredí Internetu si ako jeden z predpokladov tejto práce vypožičiame paradigma rozvedenú Polčákom, ktorý poníma právo v teórii ako „informačný systém“¹⁷. Vo svojich viacerých publikáciách túto teóriu zhŕňa ako teoretickú reflexiu organizačného charakteru systému právnych pravidiel, ktoré predstavujú súbor štátnych informácií organizujúcich život ľudských spoločností. Právne procesy vo vnútri systému spoločnosti majú charakter zberu, spracovania a distribúcie právnych informácií¹⁸. Práve tieto informácie vnášajú do ľudského spoločnosti, ktoré existuje i v pomyslenom kyberpriestore mieru organizovanosti. Našou úlohou je bádať či regulačné mechanizmy organizácie informačnej spoločnosti, ktoré predkladá štát v platnom práve sú spôsobilé znížiť entropiu v kybernetickej spoločnosti, teda i nastoliť otázku, aký spôsob regulácie, či aké právo je nielen legitímne, ale i skutočne efektívne.

1.1 „Taxonómia“ Internetu

Pre zodpovedanie hlavných téz tejto diplomovej práce si musíme položiť otázku: „čo je to internet a ako prístupit' k jeho regulácii vo sfére uvažovania verejného práva

¹⁵ WIENER, Norbert. *The human use of human beings: cybernetics and society. With a new Introduction by Steve J. Heims*. London: Free Association, 1989. ISBN 1853430757. s.12

¹⁶ WEINER, Norbert, 1989, op. cit, s.21

¹⁷ POLČÁK, Radim. *Informační teorie práva*. In *Komunistické právo v Československu*. 1. vyd. Brno: Masarykova Univerzita, 2009. s. 167-176. Mezinárodní politologický ústav. ISBN 9788021048447

¹⁸ POLČÁK, Radim. *Informační teorie práva* [online]. Masarykova univerzita. Učebné materiály predmetu Kritická právní teorie, 2008. s.7 a násl. [cit. 5.4.2018]. Dostupné z: is.muni.cz/el/1422/jaro2008/MVV012468K/um/5626625/polcak-informacni_teorie_prava.pdf

a obdobných obmedzení nastavených demokratickou spoločnosťou?“. Predpokladom uchopenia legitimacy regulácie právom je predovšetkým samotná otázka definície jej objektu – internetu ako regulovaného systému. Ako uvádza Knapp, predpokladom regulácie je: „*znalosť spoločenských vzťahov, na ktoré má právo pôsobiť a znalosť skutočného stavu, na ktorý má právna norma pôsobiť, rovnako ako žiadúceho cieľového stavu, ktorý má byť pôsobením právnej normy spôsobený*“¹⁹. Bez zodpovedania tohoto základného predpokladu nie je možné pochopiť ani ďalšie otázky ako sú nutnosť či samostatnosť právneho odvetvia, ktorá tento objekt reguluje a spôsob dosiahnutia odôvodnenej úrovne rigidity zapojením empirických skúseností s praxou prebádanými a známymi právnymi inštitútmi.

V tomto kontexte si musíme určiť rovinu pozitívnej úlohy štátu pri aplikácii všeobecne platných pravidiel správania v akomkoľvek novom objekte *sui generis* a zaistení štandardu ústavne zavedenej úrovne základných ľudských práv vo sfére, ktorá sa javí do značnej miery ako spoločenský priestor autoregulovaná. Vzhľadom k tomu, môžeme až s axiomatickou presnosťou tvrdiť, že regulácia musí primárne pôsobiť ako spojný znak medzi Internetom a sociálnou realitou, a to prostredníctvom určenia hraničných pravidiel pre jednotlivé subjekty vstupujúce do nového virtuálneho objektu²⁰.

Odhládnuv od hyperboly mystického spoločenstva kyberpriestoru, by sme mohli vnímať Internet len ako ďalší spôsob medzinárodnej spoločenskej komunikácie a výmeny informácií²¹, ktorý by snád' osobitnú normatívnu reguláciu nepotreboval. Avšak z hľadiska práva je na Internet nemožné nazerať výlučne ako na samostatne stojacu technickú entitu²².

¹⁹ KNAPP, Viktor. *Teorie práva*. Vyd. 1., 3. dot. Praha: C.H. Beck, 1995, 247 s. Beckovy právnické učebnice. ISBN 8071790281. s.40

²⁰ MATEJKA, Jan. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Vyd. 1. Praha: CZ.NIC, 2013, 258s. ISBN 9788090424876. s.25

²¹ EDWARDS, Lilian. a WAELDE, Charlotte. *Law and the Internet*. 3rd ed. Portland, Or.: Hart Publishing, 2009, 713s. ISBN 9781841138152. s.4

²² V technickom ponímaní je Internet: „*Globálna počítačová sieť poskytujúca rôzne informačné a komunikačné zariadenia pozostávajúce z prepojených sietí využívajúcich štandardizované komunikačné protokoly [TCP/IP viz. Bližšie v bode 1.3.1].*“ Prevzaté z online verzie Oxford Living Dictionaries. *Definition of Internet in English*. [cit. 29.3.2018]. Dostupné z: en.oxforddictionaries.com/definition/internet

Ako samostatný objekt bez akéhokoľvek užívateľského vstupu by Internet totiž merítkom užitočnosti neprešiel. Nie je hmotným, či nehmotným statkom, a nie je objektívnou právnou skutočnosťou nezávislou na ľudskom chovaní²³. Ako sme uviedli, je vytváraný jednotlivými subjektami s právnou subjektivitou prístupujúcim do nového priestoru - Internetu, ktorý je k nej sám nespôsobilý. Zaujímavým je názor Rady OSN pre ľudské práva, ktoré považuje prístup k internetu za formu slobody prejavu, a ako taká by mala byť chránená ako ľudské právo²⁴. Ako však zároveň uvádza La Rue²⁵ prístup k internetu je dvojdimenzionálnym pojmom, definovaný jednak nereštriktívnym prístupom k obsahu online a dostupnosťou prístupu k samotnej infraštruktúre informačných komunikačných technológií.

Od týchto dvoch rovín sa odvíja aj samotná rozdielna regulácia prístupu k obsahu²⁶ a stanovenia technických noriem pre fungovanie infraštruktúry siete. Tieto dve roviny sa do značnej miery z technickej podstaty obsahu regulujúcich noriem prelínajú. A teda, i keď naznačíme špecifiká kyberpriestoru a odôvodníme potrebu vzniku samostatného právneho odvetvia, ktoré tento priestor reguluje, nemôžeme tvrdiť, že by bol vzťah medzi kybernetickou realitou a normou neexistujúci. Predsa len z hľadiska právnej vedy i vo virtuálnom ponímaní spoločenskej reality právne vzťahy vznikajú, menia sa a zanikajú ako i v reálnom svete²⁷.

²³ SMEJKAL, Vladimír. *Internet a §§§*. Praha: Grada, 2001, 284s. ISBN 80-247-0058-1. s.17

²⁴ Srov. článok približujúci rezolúcie Rady OSN pre ľudské práva v dokumente pod č. A/HRC/32/L.20. SANDLE, Tim. *UN thinks internet access is a human right* [online]. Digital journal, publikované 22.7.2016 [cit. 28.3.2018]. Dostupné z: <http://www.businessinsider.com/un-says-internet-access-is-a-human-right-2016-7>

²⁵ LA RUE Frank. *Správa osobitného spravodajcu o podpore a ochrane práva na slobodu názoru a prejavu (dokument A/HRC/17/27) zo 16. mája 2011* [online]. Rada OSN pre ľudské práva, publikované 16.5.2011 [cit. 28.3.2018]. Dostupné z: daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/17/27&Lang=E

²⁶ Prístup ku a tvorba obsahu môžeme stotožniť s ponímaním Internetu ako sociálnej reality. V reálnom svete vytvárame „obsah reality“ formami spoločenského prejavu napríklad vyrobením produktu, ktorý ponúkame ostatným otvorením predajne, vytvorením kolekcie artefaktov v múzeu, či hlásaním myšlienok okoloidúcim. Tieto formy spoločenského prejavu však môžu mať odzrkadlenú formu prejavu v digitálnom priestore, ktoré v súhrne vytvárajú obsah Internetu ku ktorému prístupujeme.

²⁷ POLČÁK, Radim, ŠKOP, Martin a MACEK, Jakub. *Normativní systémy v kyberprostoru: (úvod do studia)*. Brno: Masarykova univerzita, 2005, 102 s. ISBN 8021037792. s. 11; s. 29 a násl.

1.1.1 Na obranu kyberpráva

Uvedeným nenaznačujeme, že sústredením sa na tradičné právne postuláty ako primárny zdroj práv by sme mali opomínať nové technológie Internetu ako efektívny motor ich zmien v čase²⁸, alebo úplne rezignovať na akcentovanie právnej istoty. Skutočnosť, že právo reguluje použitie technológie však podmieňuje vznik konfliktu modalít nutnosti a možnosti. V kontexte zmyslu informácie ako určovateľa organizovanosti, je použitá metóda odboru práva informáciou o tom, ako k objektu skúmania efektívne pristupovať. Ako polemizuje Polčák, systém právnych pravidiel nevyužívame ako pasívny nástroj ani ho aktívne nehodnotíme, pretože sa môžeme ocitnúť v situácii, kde odôvodnené a nutné pravidlo narazí na limity technických možností objektu regulácie²⁹. Pri zvážení vzťahu práva a informačných technológií *per se*, je správnym využitie navrhnutého pohľadu metodológie právneho pragmatizmu. Tento smer právneho myslenia vychádzajúc z pojednaní Williama Jamesa chápeme, ako: „*spôsob riešenia metafyzických sporov, ktoré by inak mohli byť nekonečné*“³⁰. Pre tento smer je typickým praktické a empirické uvažovanie a aplikácia primeraného riešenia každého nového právneho problému³¹. Ide o vykročenie na horizont možností praktického obsahu systému právnych pravidiel, ktoré premietneme do fakticity nových technológií³², za účelom ustálenia nového právneho odvetvia. Tým je právo informačných a komunikačných technológií (z anglického *Information and Communications Technology - ICT*, pozn.), ktoré však nejde obmedziť iba na internetové právo a ktoré

²⁸ BELLIA, Patricia L., BERMAN, Paul Schiff a POST, David G. *Cyberlaw: problems of policy and jurisprudence in the information age*. St. Paul, MN: Thomson/West, 2003, 704s. ISBN 0314144129. s.207

²⁹ POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, edice Téma, 2012, 392 s. ISBN 9788087284223. s.56 a násl.

³⁰ JAMES, William. *Pragmatism. A new name for some old ways of thinking*. Lecture II. – What Pragmatism means? [online]. Project Gutenberg, [cit. 29.3.2018]. Dostupné z: www.gutenberg.org/files/5116/5116-h/5116-h.htm#link2H_4_0004

³¹ POSNER, Richard A. Response, Legal Pragmatism Defended. *University of Chicago Law Review*. roč. 2004, č. 71.2, s. 683-690. ISSN 1939-859X

³² V našom prípade Internetu ako ohraničenia kyberpriestoru, pozn.

vhodnejšie označíme ako „kyberprávo“³³. Vzhľadom k uvedenému sme v kontexte nového prostredia nútení metodologicky pristúpiť k otázkam o tom, čo je právom, ako je tvorené a či je spôsobilé meniť spoločenské vzťahy v čase. Koncept tohoto medziodvetvového práva nestojí ako statický súbor pravidiel tvoriaci jednotný rámec regulácie vzťahov na internete, ani ako paralelné špecifické právo, naopak vyvierajúce právne problémy posudzujeme pragmaticky za pomoci konvergenzie bezmála všetkých tradičných právnych odvetví.

Diskusia za a proti štúdiu a preskúmvaniu kyberpráva sa odohrala ešte v roku 1996 medzi Easterbrookom a Lessigom, v ktorej Easterbrook pristúpil ku kyberprávu so zdanlivo uváženým odmietnutím. Vo svojej práci upozornil na riziká plytkosti využitia dynamicky sa meniaceho neunifikovaného práva, ktoré sa javí ako „*multidisciplinárny diletantizmus*“. Argumentuje, že spôsob ako sa „*naučiť právo uplatniteľné na špecializované úsilie, je štúdium všeobecných princípov práva*“, teda štúdium „*odborov, ktoré právo celistvo osvetľujú*“ následne náležite aplikovať ako napríklad „*práva duševného vlastníctva na počítačové siete*“³⁴. Jeho pohľad sa nám prvotne javí ako logická a rigidná analýza. Poukazuje v skratke na to, že vytvorením zdravých všeobecných pravidiel regulácie a presadzovania modelového správania, sa nám otvorí cesta uplatnenia týchto pravidiel na nové objekty práva ako napr. na počítačové siete. Samostatnosť náuky o práve

³³ ICT je zastrešujúcim pojmom pre technológie určené k spracovaniu a komunikácii informácie. Odvodené právo nespočíva teda iba v regulácii internetu, ktorú môžeme označiť za jednu z jeho ťažiskových pod-oblastí, taktiež je sem treba zaradiť softwarové a databázové právo rovnako ako právo ich licenčného využívania rovnako ako telekomunikačné právo. srov. napr. GRAHAM J. H. SMITH. *Internet Law and Regulation*. 4. ed. London: Sweet & Maxwell, 2007, 1374 s. ISBN 9780421909908. s.37; alebo viac ku schéme nového odboru napr. JANSÁ, Lukáš, Petr OTEVŘEL, Jiří ČERMÁK, Petr MALÍŠ, Petr HOSTAŠ, Michal MATĚJKA a Ján MATEJKA. *Internetové právo*. Brno: Computer Press, 2016, 432s. ISBN 9788025146644. s.21. Podotkneme, že sa názory na použitie výrazov *ICT* a *Cyberlaw* rôznia, kdežto angloamerický systém ich často ztotožňuje, v európskom ponímaní sa termín *kyberprávo* nepoužíva bežne. V našej práci ho využijeme prevažne pre označenie teórie internetového práva, keďže vzhľadom k dogme „Internet je hranicou kyberpriestoru“ sa javí ako konštrukčne exaktnejší pojem. Inými slovami nás *pro futuro* neobmedzuje zavedená hranica Internetu pri stanovení regulácie.

³⁴ EASTERBROOK, Frank H. *Cyberspace and the Law of the Horse*. University of Chicago Legal Forum, Roč. 1996, s.207-216 ISSN 0892-5593, citácie s. 207 a 208

kybernetického priestoru sa teda javí ako zbytočné úsilie. Realita však spočíva v tom, že názor Easterbrooka hrubo podcenil technické aspekty prispôsobovania všeobecných zákonov kybernetickému priestoru. Keby sa skutočne pokúsil dôsledne aplikovať všeobecné zákony na kybernetický priestor o niekoľko rokov neskôr, pravdepodobne by zistil, že v dynamickom prostredí zmien je taký postup prinajmenšom nedôsledný. Lessig vidí svoju odpoveď v eseji *“The law of the horse: What cyberlaw might teach”* (Koňské právo, alebo čo nás kyberprávo môže naučiť, pozn. preklad) ako úctyhodný nesúhlas s Easterbrookom. Avšak, z pohľadu našej práce, v skutočnosti obe tézy pracujú ruka v ruke pri určovaní prostriedkov, ktoré môžu kybernetický priestor regulovať. Easterbrook nechýboval v tom, že ak spoločnosť vstupuje do kybernetického priestoru, zavedená regulatívne pravidlá stanovené všeobecným právom by nemali byť len preto odlišné. Lessig však správne poukazuje na skutočnosť, že: *“tieto pravidlá v reálnom priestore závisia od určitých vlastností dizajnu reálneho priestoru”*³⁵.

Realita architektúry kybernetického priestoru (ako je navrhnutá kódom, pozn.³⁶) sa od *reálneho priestoru* líši mnohými spôsobmi, ktoré by z dôsledného zavedenia všeobecných pravidiel do kyberpriestoru robili cvičenie v analogickej interpretácii. Zložitosť regulácie architektúry kyberpriestoru, ako uvádza Lessig, pramení z jej rozdielného kódovania „informácií“ prenesenými z reálneho sveta. Napríklad prístup používateľa do kyberpriestoru umožňuje jeho virtuálnu anonymitu. Spôsob, ktorým je architektúra kybernetického priestoru kódovaná vytvára akúsi novú formu zrkadlovej spoločnosti, na ktorú sa ale stále aplikujú obmedzenia, ktoré sú v spoločnosti zaužívané ako modality regulácie správania. Tieto štyri modality aplikované súčasne i v kyberpriestore sú: *zákon, sociálne normy, ekonomický trh a architektúra sveta*³⁷. Na základe chápania toho, ako sa architektúra kybernetického priestoru líši od *reálneho priestoru*, sa vyžaduje prispôbenie všeobecných pravidiel správania buď:

³⁵ LESSIG, Lawrence. *The Law of the Horse: What Cyberlaw Might Teach*. Harvard Law Review. 1999, roč. 113, č. 3, s. 501-549. ISSN 0017-811X. s.504

³⁶ Bližší výklad Lessigovho chápania architektúry kyberpriestoru ako kódu v bode 2.1.1 a násl.

³⁷ *ibid.* s.507 a násl. Lessig rozumie sumou týchto modalít celkovú reguláciu siete. Uveďme príklady: Správanie subjektov nie je vyňaté z pôsobnosti autorského či trestného práva rovnako ako v reálnom svete. Sociálne normy sa v online diskusii aplikujú rovnako - ak ju niekto výrazne naruší, môže byť z diskusie odstránený.

- a) Prispôsobením zákonov v kybernetickom priestore tak, aby vyhovovali jeho jedinečnej architektúre – kódu, alebo
- b) Regulovaním architektúry kybernetického priestoru (zmenou jeho kódu) tak, aby bližšie zodpovedal reálnemu priestoru.

Lessig príkladne problematiku rozvádza, avšak pre potreby tejto práce je podstatné určiť, že samostatnosť kyberpráva spočíva v nachádzaní spôsobu, ako spolu tieto modalítity komunikujú alebo naopak sú vo vzájomnej konkurencii. Aby sa však právo mohlo prispôbiť, je predpokladom, aby boli právnici oboznámení s použitými technológiami s ohľadom na kód a architektúru kybernetického priestoru. Práve toto východisko nás pragmaticky podnecuje k vyčleneniu kyberpráva ako samostatného právneho odvetvia.³⁸

1.2 Umenie (vrchnostenskej) regulácie

Regulácia je abstraktným pojmom, ktorý predstavuje konštrukt zásahu do slobodnej činnosti subjektov na základe stanovených pravidiel za účelom dosiahnutia organizovaného a funkčného prostredia³⁹. Dôslednou aplikáciou informačného poňatia práva hovoríme o procese vstupu preddefinovanej informácie v podobe zákona do spoločenského systému za účelom dosiahnutia jeho organizovanosti. Ako uvádza Polčák, je otázkou či každé právne pravidlo predstavujúce vnesenú informáciu znižuje mieru entropie v spoločnosti⁴⁰. Právne normy totiž pôsobia na spoločnosť len vnesením informácie, že niečo má byť, nezávisle na tom či to zodpovedá skutočnému stavu v spoločnosti alebo nie, teda podliehajú iba kritériu platnosti ako atribútu existencie práva⁴¹. Regulatívnym vetám určujúcim povinnosť teda nie

Ekonomický trh reguluje cenu prístupu k určitým službám ale napríklad i určuje populárne miesta zverejnením cielennej reklamy. Architektúra sveta al. kód reguluje správanie pomocou prístupu, či jeho obmedzenia, teda rovnako ako železnica sprístupní určité miesta, iba určitý hardware či software alebo znalosť prístupového hesla sprístupní miesta v kyberpriestore.

³⁸ BELLIA, BERMAN a POST, 2003, op.cit., s.13-14

³⁹ POUPEROVÁ, Olga. *Institucionální aspekty regulace médií*. Vyd. 1. Praha: Wolters Kluwer ČR, 2016, 256s. ISBN 9788075523358. s 21

⁴⁰ POLČÁK, *Internet a proměny práva*, 2012, op. cit., s. 23-26.

⁴¹ KNAPP, 1995, op. cit. s.56

je pridelené kritérium ich pravdivosti. Avšak samotná skutočnosť, že právo existuje a platí nezaručuje organizovanosť spoločenského celku, teda miera regulácie a organizácie nie je od seba kauzálna závislá. Pod reguláciou si tradične predstavíme normy verejného práva vytvárané autoritatívnym subjektom primárne za účelom ochrany verejného záujmu. Postup štátu ako regulátora vynucujúceho platné právo je v tomto prípade samozrejme implicitne ospravedlnený, avšak popri otázke legitimacy je na mieste i otázka kvality a potreby autoritatívnej regulácie ako prostriedku organizácie spoločnosti. Základnou otázkou, ktorá sa nám otvára je opodstatnenie vzťahu medzi použitým prostriedkom a sledovaným cieľom regulácie. Použijeme slová Lessiga: „*Právo by malo regulovať určité oblasti kultúry, ale malo by regulovať kultúru iba tam, kde je taká regulácia dobrá*“⁴². V zásade sa zhodne snaží poukázať na prístup, v ktorom by sa mal regulátor pri rozširovaní svojej pôsobnosti *ex ante* pýtať, či bude regulácia prospešná a dobrá sledovanému cieľu. I keď sa tento prístup javí až jednostranne liberálny, spoločne s naším krátkym výkladom nás podnecuje k určení efektívnej autority, alebo pri naviazaní na Sokrata, subjektu skutočne nadaného pomyselným umením riadenia v kyberpriestore. Tým sa odpútavame od zábran istoty a stability metodológie právneho pozitivizmu a v nadväznosti na teleologický prínos Karela Engliša⁴³ sa kriticky rovnako pýtame „Prečo?“ „Pre aký účel je to dobré?“.

K určení skutočnej autority znižujúcej stav entropie v kyberpriestore zohľadníme metódy, ktoré môžeme k jeho organizácii použiť. Polčák ich odvodzuje zo zbierky prednášok

⁴² LESSIG, Lawrence. *Free Culture: How Big Media uses Technology and the Law to Lock Down Culture and Control Creativity*. New York: The Penguin Press, 2004. ISBN 1594200068. s.305. Dostupné i online z: www.free-culture.cc/freeculture.pdf

⁴³ ENGLIŠ, Karel. *Kritika normativní theorie právní*. In KOSEK, Jan, WEINBERGER, Ota a KUBEŠ, Vladimír, ed. *Brněnská škola právní teorie: (normativní teorie)*. Praha: Karolinum, 2003. ISBN 8024606895. s. 203 a násl.

o procesoch v žijúcich organizmoch Erwina Schrödingera⁴⁴ ako anarchické a regulačné⁴⁵. Prenesením tohto rozdelenia do sociálnych štruktúr zistíme, že anarchická⁴⁶ metóda je postavená na predpoklade samoorganizačných schopností spoločnosti⁴⁷, regulačná je závislá na organizačných schopnostiach externej autority – štátu ako regulátora. Aby však obidva princípy skutočne spoločenský systém organizovali, musia vychádzať nielen z jeho znalosti ale i sledovať legitímny účel každou vnesenou informáciou.

V prípade regulačnej metódy, je zjavným účelom ochrana legitímneho verejného záujmu založeného na konsenze rôznych spoločenských požiadaviek⁴⁸. Normatívne pravidlá sú ako primerané prostriedky regulácie do spoločnosti implementované externe. Informácie do systému vnáša z pozície autority štát a odvodené inštitúcie. Tým sa silami stojacimi mimo regulovaný systém, ako uvádza Hayek, vytvára produkt tejto metódy - poriadok (tiež „vytvořený řád“⁴⁹ pozn.). Touto metódou je tvorená tradičná vrchnostenská regulácia.

⁴⁴ SCHRÖDINGER, Erwin. *What is life?: the physical aspect of the living cell*. New York: Cambridge University Press, 1992. ISBN 0521427088. Práca sa našej tézy dotýka skôr okrajovo. Odvolávame sa na 1. a 6. kapitolu knihy; popis druhého termodynamického zákona – rastúcej entropie, princíp organizácie z chaosu a princíp negatívnej entropie, ktorý veľmi zjednodušene popisuje vyhýbanie sa rozkladu organizmu udržiavaním negatívnej entropie – informácie.

⁴⁵ POLČÁK, *Internet a proměny práva*, 2012, op. cit., s. 88

⁴⁶ I keď pojem „anarchická“, by snád' najvhodnejšie odpovedal ideám pionierov Internetu, budeme v tomto ponímaní pracovať skôr s praktickým pojmom „autoregulačná či samoregulačná metóda“.

⁴⁷ Spoločnosť sa ako systém bráni úpadku autonómnym vytváraním informácií. V tomto prípade má informácia normatívny charakter odvodený nie od autority, ale z hľadiska jej efektivity organizovať. Tento princíp prestupuje všetkými odbormi, pozorovať ho môžeme napríklad v klasickom diele Adama Smitha „*Pojednanie o pôvode a príčinách bohatstva národov*“ a jeho teórie neviditeľnej ruky trhu, ktorá zachytáva predstavu, že snaha jednotlivca o vlastný prospech môže byť pre spoločnosť prínosnejšia ako keby bol jednotlivec vedený snahou prospieť verejnému záujmu. srov. výklad SMITH, Adam. *Pojednání o podstatě a původu bohatství národů*. Přeložil Vladimír IRGL, Alena JINDROVÁ, Josef PYTELKA a Sergej TRYML. Praha: Liberální institut, 2016, 872 s. ISBN 9788086389608. s. 397-398

⁴⁸ POUPEROVÁ, 2016, op.cit., s.24

⁴⁹ HAYEK, Friedrich August von. *Právo, zákonodárství a svoboda: nový výklad liberálních principů spravedlnosti a politické ekonomie*. Přeložil JEŽEK, Tomáš. Praha: Prostor, 2011. Obzor (Prostor), 558 s. ISBN 9788072602537. s. 59.

Naproti tomu stojí autoregulačná metóda, ktorá stojí na slobodnej autonómii jednotlivca podriaďiť sa určitým pravidlám tam kde „štátna autorita nie je dosť dobre možná alebo dostupná“⁵⁰. Obsah a účel autoregulačných pravidiel vytvárajú činitelia odlišní od štátnej autority. Výsledkom je samoregulácia, ktorá tiež existuje iba pod akousi pomyselnou strechou autority verejného práva, ktoré ju nezakáže alebo do nej inak nevstúpi. Obdobne sa formuje seba-utvárajúci „vyrostlý rád“, ktorý Hayek nazýva abstraktné spontánnym poriadkom, teda takým, ktorý sa pragmaticky adaptuje na okolnosti. Ten sa však vo vzťahu k účelu vymedzuje nasledovne: „*Keďže takýto poriadok nebol vytvorený nejakým vonkajším činiteľom, nemôže mať poriadok ako taký taktiež žiadny účel, avšak jeho existencia môže byť veľmi užitočná jednotlivcom, ktorí sa vnútri tohto poriadku pohybujú*“⁵¹. Z citátu môžeme odvodiť, že i keď sa koncept spontánneho poriadku nedá stotožniť so samoreguláciou, ktorá má vonkajšieho činiteľa ktorým nie je štát, majú určitú súvisť. Úspech spontánneho poriadku v spoločnosti vznikne iba selektívnym vývinom pravidiel, ktoré podnietia jednotlivca k spolupráci, teda k tomu, aby sa choval spôsobom, ktorý umožňuje spoločenský život ostatným – inak z neho môže byť vyradený, alebo spoločnosť ako celok neuspeje. I keď sa pôvod pravidiel spočiatku nepochybne utváral spontánne, je predstaviteľné, že pri ich formovaní sa vytvoril nový poriadok, ktorý spočíval v uvedomelej organizácii – vytvorenom poriadku⁵².

1.2.1 Konštrukčné atribúty regulácie

V právne praktickej rovine môžeme na reguláciu nazerať optikou dvoch súperiácií podmienok, kontroly a slobody. Regulátor môže ponechať organizáciu činnosti plne na diskrecii podnikateľských subjektov sledujúcich vlastné záujmy, alebo sa zasadiť imperatívnou reguláciou o nasmerovanie týchto záujmov k prospechu spoločnosti ako

⁵⁰ POUPEROVÁ, 2016, op.cit., s.29

⁵¹ HAYEK, 2011, op.cit., s.62 a násl.

⁵² *ibid*, s.68 a násl.

celku⁵³. Avšak dichotómia absolútnej kontroly alebo slobody subjektov je značne nepružná, preto spoločnosť začala hľadať alternatívy k tradičnej regulácii. Produktom tohoto prístupu je samoregulácia⁵⁴, alebo dosiaľ nespomenutá alternatíva tzv. metaregulácie⁵⁵.

K pochopeniu týchto pojmov určíme štyri základné atribúty akéhokoľvek regulačného prístupu ako: *subjekt regulácie, regulátor, príkaz a dôsledok*⁵⁶. Pod *subjektom regulácie* rozumieme primárne entitu na ktorú sa regulácia vzťahuje a na ktorú budú aplikované dôsledky nepodriadenia sa. *Regulátor* je autoritatívna entita⁵⁷, ktorá určuje a presadzuje regulatívne pravidlá. Pod tými rozumieme *príkazy*, ktorými regulátor určuje, aby subjekt regulácie niečo vykonal alebo sa naopak určitej činnosti zdržal. Tie rozdeľuje Coglianese a Mendelson na príkazy určené cieľom, ktorý má byť dosiahnutý (zodpovednosť za finálny stav) a prostriedkami, ktoré taký cieľ majú dosahovať (napríklad implementácia novej technológie). Výsledkom plnenia príkazu subjektom regulácie je *dôsledok* – negatívny (v podobe správnej pokuty) alebo pozitívny (exempcia z určitej povinnosti). Z dôsledkov jednotlivých atribútov pre túto prácu stačí.

Charakteristickým rysom samoregulácie je unifikácia entity regulátora a subjektu regulácie. Subjekt aplikuje a presadzuje vlastné či profesné príkazy smerom do vnútra svojej štruktúry. Výlučné použitie tohto prístupu je v prostredí Internetu snád' iba silne idealistickou predstavou, ako sme uviedli Internet sa za samostatný subjekt nedá pokladať. Mohli by sme skôr uvažovať o subjekte poskytujúcem aplikácie či služby v sieti, ako regulátorovi aktivít užívateľov jeho produktu. Prínosom nie je teda len efektivita či rýchlosť, ale často súbežná

⁵³ BALDWIN, Robert, CAVE, Martin a LODGE, Martin ed. *The Oxford handbook of regulation*. Vyd. 1. Oxford: Oxford University Press, 2010. ISBN 9780199560219. s.146

⁵⁴ COGLIANESE, Cary. a KAGAN, Robert A. *Regulation and regulatory processes*. Burlington, VT: Ashgate, 2007, 752 s. ISBN 9780754625186. s.22

⁵⁵ Pojem napr v DRAHOS, Peter ed. *Regulatory theory : foundations and application*. Acton, AU: ANU Press, 2017. ISBN 9781760461027, s. 149 a násl.

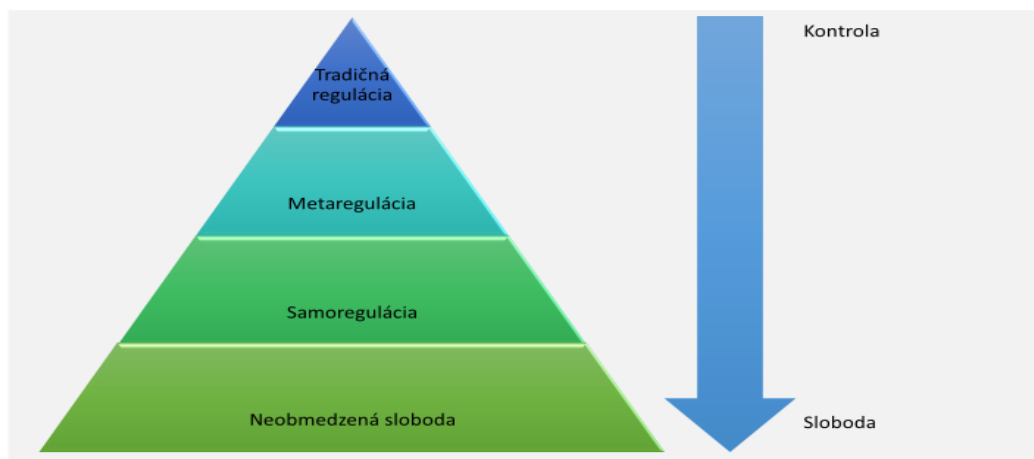
⁵⁶ Delenie a výklad jednotlivých atribútov prevzatý z: BALDWIN, CAVE a LODGE ed., 2010, op.cit., s.148 a násl.

⁵⁷ Ako sme naznačili nemusí sa nutne v rozdielnom prístupe k regulácii jednať o štát a odvodené inštitúcie, pozn.

aplikácia etických štandardov správania sa, ktoré presahujú znenie zákona⁵⁸. Príkladom by mohla byť moderované diskusné fórum na webových stránkach. Účelom či skôr motiváciou stanovenia týchto pravidiel nad rámec zákona samoregulovaným subjektom je primárne odvrátenie zásahu vrchnostenskej regulácie⁵⁹.

Metaregulácia je skôr kontrastným prístupom medzi samo a vrchnostenskou reguláciou. Regulátor je v tomto prípade najčastejšie autoritatívny štát, ktorý vyhradzuje určitú kostru regulácie *prikazmi*, ktorých implementáciu často ponecháva na diskrecii regulovaného subjektu, ktoré ju dobrovoľne prijímajú pod pomyselnou hrozbou prechodu na striktnú vrchnostenskú reguláciu. Ide o obojstranne výhodný vzťah, v ktorom regulátor dáva subjektu vyššiu mieru voľnosti pri implementácii⁶⁰ regulácie a súčasne nemusí dôkladne riešiť vyvstávajúce technické otázky. V kyberpriestore, ako poukážeme vo viacerých častiach práce je, alebo by mal byť tento prístup základným východiskom zaručujúcim symbiotické súžitie odlišných častí spoločenského systému.

Popísanú dynamiku prechodu v diskrečnej voľnosti regulovaného subjektu od kontroly k slobode v metódach regulácie názorne ilustruje Coglianese a Mendelson⁶¹:



Pyramída diskrečnej voľnosti subjektu regulácie

⁵⁸ GUNNINGHAM, Neil, REES, Joseph. Industry Self-Regulation: An Institutional Perspective. *Law&Policy*. 1997, Roč. 19, č. 4, s. 363-414. ISSN 0265-8240. s.366

⁵⁹ POUPEROVÁ, 2016, op.cit., s.31

⁶⁰ BALDWIN, CAVE a LODGE ed., 2010, op.cit., s.151

⁶¹ Prevzaté s prekladom autora. BALDWIN, CAVE a LODGE ed., 2010, op.cit., s.152

1.3 Kontext histórie Internetu

Ako vyplýva z vyššie uvedeného, jedným z obsahových východísk kyberpráva je dynamické prispôsobovanie sa či premeny zákonov a postojov odbornej verejnosti v čase. Samotnému odboru však absentuje privilégium zatriedenosti a ustálenosti tradičných právnych disciplín. K porozumeniu vyčlenených problémov kyberpráva, či ďalej regulatorným východiskám blokovania prístupu k obsahu internetu, je dôležité aspoň v hraničných kontúrach priblížiť krátku dobu existencie internetu s cieľom objasniť počiatky informačnej revolúcie v spoločnosti a východiskové nadšenie a hodnoty tvorcov, ktoré ovplyvnili vznik a vývoj právnej disciplíny, ktorú so sebou tento celospoločenský fenomén priniesol.

Internet svojím významom predstavuje jeden z najúspešnejších príkladov prínosov trvalých investícií a záväzku výskumu a vývoja informačnej infraštruktúry. Od začiatku výskumu v oblasti paketového prenosu⁶² boli vláda, priemysel a akademická obec partneri v rozvíjaní a nasadzovaní novej technológie, ktorá sa postupom času stala neodmysliteľnou súčasťou fungovania štátnych, ekonomických a technologických subjektov.⁶³

1.3.1 Počiatky Internetu

Za pioniera myšlienkového zdroja technológie, ktorú dnes nazývame internetom, je považovaný Joseph Carl Robnett Licklider, profesor prestížneho amerického MIT⁶⁴, ktorý niekoľkými správami v roku 1962 popísal koncept decentralizovanej siete prepojujúcej vojenské objekty za účelom zrýchlenia komunikácie, neskôr rozvinutý zámerne grandióznou

⁶² Packet Switching – „spôsob prenosu údajov, v ktorom je správa rozdelená na niekoľko častí, ktoré sú odosielané nezávisle na ľubovoľnej trase optimálnej pre každý paket a sú opätovne zostavené do celistvej správy na mieste doručenia“. Prevzaté z INSTITUTE, Government. Telecommunications: glossary of telecommunications terms. Rockville, Md: Government Institute, 1998. ISBN 9780865875807, str. P-1

⁶³ LEINER, Barry M. *Brief History of the Internet* [online]. Internet Society, publikované 1997 [cit. 5.11.2017]. Dostupné z: www.internetsociety.org/internet/history-internet/brief-history-internet/

⁶⁴ Massachusetts Institute of Technology, pozn.

tézou o „*Intergalactickej Počítačovej Sieti*“⁶⁵, spočívajúcej v prepojení niekoľkých počítačov za účelom rozdelenia pamäte v režime takzvaného „time-sharing do jednotnej siete“⁶⁶. Na základe tohto nadčasového konceptu bol menovaný do čela *Information Processing Techniques Office* a agentúry pre výskum obranných projektov (Defense Advanced Research Projects Agency - DARPA, pozn.). Vízia Galaktickej Siete bola v roku 1969 pretvorená do svojej prvej primitívnej podoby projektom ARPANET, ktorý umožnil výmenu dát medzi jednotlivými počítačmi zapojenými v tejto sieti⁶⁷.

Otvorené protokoly prenosu vyvinuté vedcami v DARPA sú dodnes vo veľkej miere zodpovedné za prenos informácií na sieti, čo môžeme pripísať primárnym zásadám pokroku v rannom akademickom prostredí, teda otvorenosť informácií a zdieľanie výsledkov. Ďalším vývojom internetovej siete sa v osemdesiatych rokoch zaoberala Národná vedecká nadácia (National Science Foundation - NSF, pozn.), americká nezávislá vládna agentúra, ktorá v roku 1981 ponúkla 5-ročný rozpočet pre vývoj projektu k nezávislej sieti CSNET⁶⁸, ktorá by prepojila ARPANET a ďalšie paketové siete, cez ktoré by bolo možné prepojiť akademické centrá informatiky univerzít naprieč kontinentom Spojených štátov amerických a neskôr sveta⁶⁹. Sieť CSNET premostila včasný výskum paketového prenosu až po prepojenie siete na základe vhodne zvolenej infraštruktúry, čo vybudovalo rozsiahlu prepojenú akademickú

⁶⁵ LICKLIDER, J.C.R. *The Intergalactic Computer Network: Topics for Discussion at the Forthcoming Meeting* [online]. Publikované: 23. 4. 1963 [cit. 5.11.2017]. Dostupné z: www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network

⁶⁶ NORMAN, Jeremy M. *From Gutenberg to the Internet: a sourcebook on the history of information technology*. Novato, CA: Historyofscience.com, 2005. ISBN 0930405870. s. 91

⁶⁷ PELKEY, James. *Entrepreneurial Capitalism and Innovation: A History of Computer Communications 1968-1988* [online]. Chapter 2 Intergalactic Vision to Arpanet. Publikované 2007 [cit. 30.3.2018]. Dostupné z: www.historyofcomputercommunications.info/Book/2/2.1-IntergalacticNetwork_1962-1964.html

⁶⁸ Computer Science Research Network, pozn.

⁶⁹ DENNING, P.; HEARN, A.; KERN, C.W. *History and Overview of CSNET* [online]. Publikované 12/1982 [cit. 7.11.2017]. Dostupné z: pdfs.semanticscholar.org/adae/a5be633869d79dfd6f6f23f5aa09cee92860.pdf.s.8

komunitu spolupracujúcu s priemyslom a vládnymi inštitúciami. Práve týmto prerodom v realizácii prenosu dátujeme tvorbu prvotnej univerzálnej siete internetu⁷⁰.

K zaisteniu fungovania siete pri plánovanej záťaži, bolo potrebné umožniť komunikáciu medzi existujúcimi sieťami (ARPANET a CSNET, pozn.) zjednotením protokolov jednotlivých paketových sietí a ich rozhrania s koncovými počítačmi ako i zabezpečiť vyššiu prenosovú kapacitu⁷¹. Unifikačným komunikačným nástrojom sa stal protokol TCP/IP⁷². Prepojením sietí na základe TCP/IP protokolu bola vytvorená výkonnejšia sieť pomenovaná National Science Foundation Network (NSFNet, pozn.), ktorou výstavba počítačových sietí prekročila hranicu medzi vedou a spoločnosťou o ktorej s nemalou hyperbolou hovoríme ako o dobe vedeckej transformácie sveta, ktorá otvorila cestu Internetu v modernom poňatí jeho veľkosti a dosahu.

Existenciu siete NSFNet doplnilo spustenie služby Internetu World Wide Web v roku 1991 v Európskej spoločnosti pre jadrový výskum⁷³ vo Švajčiarsku, vystavanej na princípe hypertextovej databázy s vloženými odkazmi - informáciami, ktoré môžu byť ďalej vyhľadávané a zdieľané užívateľmi po zadaní identifikátora umiestnenia informácie na *Webe*⁷⁴. K tomu slúži tzv. URL (Uniform Resource Locator, pozn.), čo je zjednodušené povedané - identifikátor adresy informácie a protokolu, ktorú stačí zadať do prehliadača *Webu* alebo kliknúť na jej odkaz a požadovaná informácia sa sprístupní⁷⁵.

⁷⁰ LANDWEBER, Lawrence. *The Computer Science Network. Asian Internet History Project* [online]. CSNET, publikované: 7.6.2012 [cit. 7.11.2017] Dostupné z: sites.google.com/site/internethistoryasia/book1/3-2-csnet

⁷¹ Seriál „Jak na Internet“. *Diel 4.5 Historie Internetu* [online]. Publikované v r. 2012-2014 [cit. 9.11.2017]. Dostupné z: www.jaknainternet.cz/page/1205/historie-internetu/

⁷² Transmission Control Protocol/Internet Protocol. „*Je to súhrn sieťových protokolov, ktoré dovoľujú vzájomným použitím dvom a viacerým počítačom komunikovať*“. MITCHELL, Bradley. *Understanding Transmission Control Protocol/Internet Protocol (TCP/IP)* [online]. lifewire, publikované: 10. 06. 2017 [cit. 9.11.2017]. Dostupné z: www.lifewire.com/transmission-control-protocol-and-internet-protocol-816255

⁷³ CERN - Organisation européenne pour la recherche nucléaire, pozn.

⁷⁴ LEE, Tim Berners. *The World Wide Web: Past, Present, Future* [online]. W3, publikované v 8/1996 [cit. 25.3.2018]. Dostupné z : www.w3.org/People/Berners-Lee/1996/ppf.html

⁷⁵ W3C. *Architecture of the World Wide Web, Volume One* [online]. Publikované 15.4.2004 [cit. 30.3.2018]. Dostupné z: www.w3.org/TR/webarch/

V oblasti regulácie je považovaný jeden z jeho tvorcov sir Tim Berners-Lee za advokáta tzv. Net Neutrality⁷⁶, bezplatného oprávneného prístupu a minimum spätnej kontroly na ktorom bol World Wide Web vystavaný. I k dnešným pomeroch sa súčasťou javí citácia tvorca: „(..Technológia takého významu..) nemôže byť navrhnutá v univerzálnom priestore a súčasne byť pod kontrolou“⁷⁷.

1.3.2 Podiel súkromných subjektov na vývoji modernej internetovej siete

Transformácia internetu do jeho súčasnej podoby začala zvoľna v polovici deväťdesiatich rokov pri predstavení prvej vysokorýchlostnej siete vBNS⁷⁸, ktorá umožnila prvý prístup súkromným subjektom odlišným od vzdelávacích inštitúcií. Tieto subjekty museli preukázať také technologické vybavenie, ktoré bolo schopné uniesť spomínanú záťaž siete, a zároveň sa na nej podieľať. Práve touto dobou začalo komerčné využívanie siete internetu, ktoré NSFNet pretvorený na Internet pôvodne nepovoľoval tak ako ho poznáme dnes.

Toto obdobie môžeme súhrnne nazvať dobou „komercializácie služieb internetu“, ktoré poznamenalo odstránenie komerčných obmedzení zavedených NSF, ako jednej z regulujúcich entít, vznik služby World Wide Web a užívateľsky dostupných prehliadačov a rýchly vstup veľkého počtu súkromných subjektov⁷⁹, ktoré pri popularite, s akou sa internet rozvíjal, rýchlo zachytili jeho enormný ekonomický potenciál, ktorý sa ešte navýšil v roku 1999, keď spoločnosť MCI, zodpovedajúca za technické prevedenie a údržbu vBNS, predstavila modul spočívajúci vo voľnejšom výbere užívateľov pripojených nezávisle na schválení poskytovateľom siete⁸⁰.

⁷⁶ Bližšie k pojmu a princípu v úvode časti 4.

⁷⁷ World Wide Web Foundation. *History of the Web* [online]. [cit. 10.11.2017] Dostupné z: webfoundation.org/about/vision/history-of-the-web/

⁷⁸ Very High-speed Backbone Network Service, pozn.

⁷⁹ JAFFE Adam B.; LERNER Josh; STERN Scott. *Innovation policy and the economy*. Cambridge, MA: National Bureau of Economic Research, 2001. ISBN 9780262600415. s. 152

⁸⁰ BREIDENBACH, Susan. Future of High Speed Networks. *NetworkWorld*. 2000, roč. 17, č. 7, s. 67-68. ISSN 0887-7661.

V priebehu deväťdesiatich rokov zaznamenal projekt NSFNET a neskoršia báza vBNS+ prerast v samo-riadiacu sa entitu⁸¹, dosiaľ neuchopenú právnym rámcom. Jediným smerodajným dokumentom boli tzv. „Podmienky prípustného využitia“⁸². Išlo o pravidlá pre používanie internetu vytvorené poskytovateľom siete, v tomto prípade NSF s odkazom na MCI vzťahujúcim sa na všetky subjekty pripojené k sieti. Tento dokument bol postavený na základe zmluvy s koncovým užívateľom, nie nepodobný dnešnému systému zmlúv s poskytovateľmi pripojenia k sieti, na rozdiel od ktorého však „*chýbala priama vymáhateľnosť na základe zákona, nakoľko využitie internetu nebolo dostatočne normatívne definované*“⁸³.

Komercializáciou internetu a s rastúcim počtom komerčných subjektov podieľajúcich sa v časovom ohraničení deväťdesiatich rokov vlády členských štátov Európskej Únie a medzinárodné organizácie čelili výzve zakotvenia jednotného regulačného rámca pre Internet, ktorý by umožnil národným štátom realizovať nielen jeho enormný ekonomický potenciál, ale aj obmedziť jeho zneužívanie⁸⁴. EÚ prešla v ponímaní nutnosti regulácie v období od roku 1991 značným posunom od obhajovania vládnej regulácie k obhajobe samoregulácie⁸⁵, pri ktorej v modifikovanej miere zotrvala. Musíme podotknúť, že Internet bol spočiatku na okraji legislatívneho úsilia EÚ a členských štátov, kde najvýznamnejším, takmer päť ročným úsilím je súbežne s pretvorením internetu z akademickej siete na komerčnú sieť svetového rozsahu, prijatie smernice Európskeho parlamentu a Rady 95/46/ES z dňa 24. októbra 1995 o ochrane fyzických osôb v súvislosti so spracovaním osobných údajov a o voľnom pohybe týchto údajov. Sústreďenie na zachovanie zavedených práv občanov EÚ, najmä súkromia a vlastníctva, je viditeľné i v následných smerniciach

⁸¹ Self-governing entity, pozn.

⁸² AUP (Acceptable Use Policy), pozn.

⁸³ GRAHAM J. H. SMITH. *Internet law and regulation*. 4. ed. London: Sweet & Maxwell, 2007. ISBN 9780421909908. s.16

⁸⁴ BONY, Elizabeth de. European Union Sees Need to Regulate 'Net. *ComputerWorld*. 1996, roč. 30, č. 43, s.90. ISSN 0010-4841

⁸⁵ FEELEY, Matthew J. EU Internet Regulation Policy: The Rise of Self-Regulation. *Boston College International and Comparative Law Review*. 1999, Roč. 22, č. 1, s. 159 – 174. ISSN 0277-5778. s.161

upravujúcich ostatné fragmentované časti práva informačných technológií prenikajúceho do komerčného obchodu⁸⁶.

História internetu v Českej republike nebola od európskej priveľmi odlišná, i keď je nutné poznamenať, že následkom politických a ekonomických faktorov, bola ČR pripojená k sieti Internet až 13.2.1992⁸⁷ na pražskom ČVUT, pričom na základe zmienených AUP, mohli sieť používať spočiatku iba nekomerčné akademické subjekty. Pripojenie Českej Republiky popisuje doc. Peterka ako „senzáciu, dešifrovanú iba malou hrstkou skutočných nadšencov“⁸⁸. V dnešnej dobe v Českej republike používa internet viac ako 9.3 milióna používateľov⁸⁹, čo v rámci Európskej Únie predstavuje nadpriemer⁹⁰.

Výraznejšie regulačné snahy sa dajú pozorovať v období vstupu ČR do Európskej Únie, ktoré sa letným pohľadom môžu javiť až ako otrocká adaptácia a preklad znenia európskych smerníc.

⁸⁶ WITZLEB Norman et al. *Emerging challenges in privacy law: comparative perspectives*. Cambridge, UK: Cambridge University Press, 2014, 470s. ISBN 9781107041677. s.261

⁸⁷ CHLAD, Radim. *Historie Internetu v České republice* [online], Publikované: r.2000 [cit. 11.12.2017]. Dostupné z: www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm

⁸⁸ PETERKA, Jiří. *Historie českého internetu: slavíme 10. výročí liberalizace*, eArchiv [online]. Publikované: 1.7.2005 [cit. 12.11.2017]. Dostupné z: <http://www.earchiv.cz/b05/b0700002.php3>

⁸⁹ Internet World Stats – Usage and Population Statistics [online]. Dostupné z: www.internetlivestats.com/internet-users/czech-republic/ ku [cit. 1.10.2017], čo odpovedá 88.4% obyvateľstva.

⁹⁰ 80,1%, pozn.

2 Teória regulácie kyberpriestoru

Už samotný vznik internetu poznamenala debata, ktorú je možné označiť ako problematiku regulácie a deregulácie kyberpriestoru v novom normatívnom obore aktivít⁹¹. Spoločnou mantrou pionierov Internetu sa v jeho ranných dobách rozhodne stalo prázdne volanie „*Neregulovať!*“. Pravda je však taká, že Internet bol regulovaný určitou autoritou vždy⁹².

V časti 2 rozvedieme koncepciu budovania architektúry kyberpriestoru, ktorá sa prelína s tvorbou a aplikáciou prebádaných východísk regulačných metód⁹³. Tým aplikujeme poznatky o modalitách regulácie do kyberpriestoru a budeme hľadať authority schopné v ňom jednotlivými prostriedkami efektívne informačnú spoločnosť organizovať. Nepôjde však iba o efektívne znižovanie entropie, ale taktiež o legitimitu tejto vnesenej informácie, teda súhrnnej odpovede na otázku „Prečo?“. Inými slovami, ak si spoločnosť sama nastaví mechanizmy regulácie nechceného správania online, pôjde o efektívne decentralizované riadenie alebo o hrozbu nelegitímneho zásahu do zavedených práv a slobôd?

2.1 Obecné úvahy o Internete, kyberpriestore a nutnosti jeho regulácie

Pojem *kyberpriestor* je charakterizovaný množstvom významov, ktoré Strate rozvádza taxonómiou "kybernetických priestorov", ktoré zjednodušene identifikuje v abstrakte na troch úrovniach. Prvá je ontológia filozofického abstraktu pojmu, ako sme ho definovali v úvode tejto práce. Druhá úroveň zahŕňa stavebné bloky, ako je fyzický koncepčný a vnemový priestor alebo virtuálny priestor a spoločne s treťou úrovňou, ktorou je ich syntéza, vrátane odrôd kybernetického priestoru, ako je mediálny priestor, estetický

⁹¹ GIBBONS Llewelyn Joseph. No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace. *Cornell Journal of Law and Public Policy*. 1991, Roč. 6, č.3, s. 475-551. ISSN 1069-0565

⁹² WEISER, Philip J. Internet Governance, Standard Setting, and Self-Regulation. *Northern Kentucky Law Review*. 2001, Roč. 28, č. 4, s. 822-846. ISSN 0198-8549

⁹³ ANDRUŠKO, Alena. *Internet, informační společnost a autorské právo*. Praha: Wolters Kluwer ČR, 2016, 276 s. ISBN 9788075523273. s.34

priestor, dátový priestor a osobný a spoločenský priestor⁹⁴. K tomuto chápaniu sa prikláňame v tejto práci a Internet definične stanovujeme ako virtuálnu syntézu technického a spoločenského ohraničenia kyberpriestoru. Takáto definícia je v zásade trúfalým počínom, nakoľko vývoj kyberpriestoru prebieha v chaotickom neukončenom procese a Internet ako kybernetická entita je nezávislá na politickom usporiadaní sveta, ktorý transcendentuje samotným substrátom. Preto sa nám za základnú tézu javí skutočnosť: „čo je platné dnes, stráca relevanciu zajtrajškom“.

Príkladom je napríklad východisko Post – Johnsonovej tézy, ktorá utopicky argumentuje, že samotná decentralizovaná štruktúra Internetu podnecuje rétoriku jeho vyňatia z územných hraníc pôsobnosti právnych inštitúcií a práva a „určiť novú hranicu kybernetického priestoru, ktorý potrebuje a môže vytvoriť vlastné nové právne a právne inštitúcie“⁹⁵. Kyberlibertariánsky idealizmus v prístupe k Internetu ako ku demokratizujúcej sile⁹⁶ v spoločnosti je snád’ najlepšie prezentovaný zakladajúcim dokumentom organizácie *Electronic Frontier Foundation*, aktívneho hnutia za slobodný Internet angažovaného v boji proti právnemu a inému obmedzovaniu slobôd užívateľov Internetu⁹⁷. Ako píše John Perry Barlow k presadzovaniu autoritatívnej aplikácie právnej regulácie v kyberpriestore v Deklarácii nezávislosti kyberpriestoru: „*Vlády priemyselného sveta, Vy unavení obri z mäsa a ocele, prichádzam z Kyberpriestoru, nového domova mysle. V záujme budúcnosti Vás, entity minulosti, žiadam, aby ste nás nechali na pokoji. Tam, kde sa zhromažďujeme, nemáte žiadnu právomoc. Nemáme volenú vládu a ani žiadnu mat’ nechceme, tak vám*

⁹⁴ STRATE, Lance. The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication*. 1999, Roč. 63, č.3, s.382-413.

⁹⁵ JOHNSON, D.R. a POST D.G. Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*. 1996, Roč. 48, č. 5, s. 1366-1402. ISSN 1939-8581. s.1367 a 1370

⁹⁶ LAIDLAW, Emily B. *Regulating speech in cyberspace: gatekeepers, human rights and corporate responsibility*. Cambridge, UK: Cambridge University Press, 2015, 356 s. ISBN 9781107049130. s.3

⁹⁷ Bližšie k histórii hnutia EFF viz. dostupné z: www.eff.org/about/history. alebo napríklad VOLLMER, Timothy. *EFF: Fighting for your digital rights for 25 years* [online]. Creative Commons, publikované 10.7.2015 [cit. 7.4.2018]. Dostupné z: creativecommons.org/2015/07/10/eff-fighting-for-your-digital-rights-for-25-years/

nepriznávam viac autority ako takú, z pozície ktorej hovorí sloboda samotná. Vyhlasujem globálny sociálny priestor, ktorý budujeme, za prirodzene nezávislý od tyranie, čo chcete na nás uvaliť. Nemáte žiadne morálne právo nám vládnuť a ani nedisponujete donucovacími prostriedkami, ktorých by sme sa naozaj báli ... Nepoznáte nás, ani náš svet. Kyberpriestor neleží vnútri vašich hraníc. ... Nepoznáte našu kultúru, našu etiku, či nepísané pravidlá, ktoré už teraz zabezpečujú našej spoločnosti viac poriadku, ako by bolo možné dosiahnuť akýmkoľvek vašimi predpismi .. Tvrdíte, že sú medzi nami problémy, ktoré musíte riešiť. Toto tvrdenie používate ako ospravedlnenie pre narušanie nášho priestoru. Mnoho týchto problémov ani neexistuje. My si sami zistíme, kde sú skutočné spory, kde sa dejú krivdy a budeme si ich riešiť po svojom. Tvoríme si našu vlastnú spoločenskú zmluvu“⁹⁸. I tento malý výsek z Deklarácie znie v súčasnosti ako nerealizovaná utopická vízia novej spoločnosti, ktorá neuzavrela spoločenskú zmluvu s tvorcom právnych noriem a ani sa jej nemieni podriaďovať. Poukazuje argumentom, že problémy v kyberpriestore nepotrebujú autoritatívny zásah, ale môžu byť riešené samoregulačne a ďalej v zmysle Post-Johnsonovej, ktorá tézy poukazuje na neschopnosť štátu obmedzeného tradičnou jurisdikciou efektívne vynucovať právo v kyberpriestore ⁹⁹. Úlohou našej práce však nie je bližšie hľadať hraničné ukazovatele pôsobnosti práva, avšak podotkneme, že takýto kyberlibertáriánsky prístup bol postupne prekonaný napríklad zavedením regulácie primárne súkromnoprávnymi zmluvami a všeobecnými pravidlami medzinárodného súkromného práva aplikovateľnými na reálny priestor.

2.1.1 Príbeh o dvoch kyber_mestách

Predstavme si dva národy - *kyber_libertariánov*, ktorí našli ideologickú oázu v novom kyberpriestore, veci s neobmedzenou schopnosťou produkovať nové informácie a národ *ludditov*, žijúci mierovo so storočiami preverenými hodnotami, morálkou a

⁹⁸ BARLOW, John Perry. *A Declaration of the Independence of Cyberspace* [online]. EFF, publikované 8.2.1996 [cit. 7.4.2018]. Plné nepreložené znenie dostupné z: www.eff.org/cyberspace-independence

⁹⁹ POLČÁK, *Internet a proměny práva*, 2012, op.cit., s.97

ideológiou¹⁰⁰. *Kyber_Libertária* prijala všetkých nových pomyselných občanov, ktorí si postupne začali časti kyberpriestoru prisvojovať a predávať ako majetok a v štáte nastal stav chaosu. Časť pomyselných občanov naďalej sprofanovane kričala: "*Informácie chcú byť zadarmo!*"¹⁰¹ Iní sa vzdali svojich utopických snov a vyrovnali sa s tým, čo videli ako nevyhnutnú realitu. Na opačnom konci sveta kybernetického priestoru žil národ *Ludditov*, nevedel veľa o kybernetickom priestore, s výnimkou toho, že má neuveriteľnú silu zbierať neobmedzené množstvo informácií, ktoré ak by prenikli do architektúry mesta *Ludditov* rozrušili by tradície, normy a morálku, ktoré od začiatku zaväzovali ich národ, a preto násilne vnikli do *Kyber_Libertárie* a snažili sa informáciu obmedziť. Uvedomovali si, že informácia ako taká nemôže byť ideológiou sama o sebe, totiž každá spoločnosť musí byť viazaná i zavedenými normami a tradíciami.

Táto možno mierne infantilne znejúca metafora predstavuje niekoľko dôležitých porozumení stretu konzervatívneho štátu a novonadobudnutej slobody, alebo tiež regulačnej a anarchickej metódy. Naproti poznatkom z kybernetiky poznávame, že sloboda *informácie* v doslovnom slova zmysle nemôže byť jediným nástrojom organizácie spoločnosti. Kybernetický priestor úplne slobodne poskytujúci informácie by mohol tiež dosiahnuť presný opak a ich komercializáciou uviesť spoločenský systém do chaosu. Avšak nedá sa ani tvrdiť, že organizuje výlučne storočná tradícia a norma, predstavujúca metaforu štátu-regulátora poskytujúcemu ochranu národa zákonom, organizačnej úlohy, ktorej sa zhostí ak sa spoločnosť vrhá do chaosu, podobne ako v prípade národa *ludditov*, ktorý *vnikol do Kyber_Libertárie*. Inými slovami, aj keď chce byť vnesená informácia slobodná, jej príjemca ako spoločenský systém musí mať nastavené externé medze chovania.

Tieto medze však nespočívajú len v podriadení sa regulácii zákonom, ale tiež iným normatívnym hodnotám, vtelených do kyberpriestoru pôvodne naznačenými v bode 1.1.1

¹⁰⁰ Metafora z knihy *Príbeh dvoch miest* od Charlesa Dickensa prevzatá celistvo z KIM, Tae. "*Free Speech*" in *Cyberspace* [online]. 1998, [cit 7.4.2018]. Dostupné z: cyber.harvard.edu/fallsem98/final_papers/Kim.html

¹⁰¹ Týmto výrokom je kreditovaný Stewart Brand v konverzácií so Steve Wozniakom, zaznamenanaj na konferencii hackerov v roku 1984. Napr. LEVY, Steven. *Hackers at 30: „Hackers“ and „Information wants to be free“*. wired, publikované 21.11.14 [cit. 7.4.2018]. Dostupné z: www.wired.com/story/hackers-at-30-hackers-and-information-wants-to-be-free/

ako *sociálne normy, ekonomický trh a architektúra*, ktorú Lessig v jeho práci nazýva *kód*. Tieto modalitty môžeme nazvať súhrnne aj *definičné normy kyberpriestoru*, ktoré vo výsledku určujú - definujú sociálny život v kyberpriestore. Kód samostatne ako obskúrný regulátor „*neviditeľnou rukou kyberpriestoru vytvára jeho [odlišnú] architektúru .. umožňujúcu perfektnú kontrolu a efektívnu reguláciu*“¹⁰². Nie sú to iba právne normy, ktoré regulujú chovanie, ale taktiež normy stanovené entitami, ktoré disponujú ostatnými modalitami regulácie a kódom ovládajúcim technologické prostriedky. Z príbehu o dvoch kyber_mestách sme dospeli k poznaniu, že samoregulatívna sloboda, po ktorej raná kybernetická komunita volala, nebola prvotne obmedzená štátom, ale ostatnými modalitami regulácie - odlišnými sociálnymi a etickými zvyklosťami nových občanov, a tých ktorí si uvedomili enormný ekonomický potenciál a začali si časti kyberpriestoru súkromne prisvojovať. Štát v takom prípade do systému autoritatívne vstúpil až keď systém začal podliehať rozmáhajúcej sa entropii. Chápanie „*dobrého libertariána*“, ktorý považoval autoritu vlády za hlavné ohrozenie slobody a vítal súkromné vlastníctvo firiem a ľudí, je v tomto prípade mylné. Je to v prvom rade nový regulátor – kód, ktorý vytvoril nepriamu hrozbu niektorým slobodám, ktoré samoregulačné metódy nevedia dostatočne kontrolovať či zabezpečiť.

2.2 Legitimita a efektivita kódu a noriem v kyberpriestore

Spomenuli sme, že kód ako neviditeľný regulátor stavia odlišnú blokovú architektúru sociálneho prostredia kyberpriestoru technickými pravidlami hardwaru a softwaru¹⁰³ „*akými sú programové obmedzenie, parametre prostredia, formáty dát, prenosové protokoly a pod.*“¹⁰⁴. Fakticita tohto kódu odlišuje jednotlivé úrovne kyberpriestoru, do ktorého užívateľ vstupuje, čím nadväzuje na abstraktné rozdelenie úrovní kyberpriestoru podľa Stratea v úvode tejto časti. Nie je ťažké si predstaviť rané kybernetické komunity, ktoré

¹⁰² LESSIG, Lawrence. *Code: Version 2.0*. New York: Basic Books, 2006, 424s. ISBN 0465039146. s.4 a 81. Publikácia je i voľne dostupná online z: codev2.cc/download+remix/Lessig-Codev2.pdf

¹⁰³ *ibid.*, s.121

¹⁰⁴ POLČÁK, *Internet a proměny práva*, 2012, op.cit., s.188

zaviedli svoje tajné pravidlá – kódy a heslá, neprístupné obyčajným návštevníkom neangažovane si prehliadajúcim úroveň priestoru Internetu¹⁰⁵. Ten ako virtuálne ohraničenie kyberpriestoru obsahuje vlastné hodnoty často náhodnému návštevníkovi úplne neznáme. I keď v sieti existujú malé, samoregujúce komunity, ich charakter je najlepšie popísaný ako anonymný a dočasný¹⁰⁶.

Aplikovateľný kód je veľmi podobný prírodným zákonom, ktoré i keď nám nie sú dostatočne známe, prirodzene pre ich adresáta platia. Naproti prírodným pravidlám sa ale kód odlišuje jeho umelou tvorbou a relatívne jednoduchou zmenou. V tomto ponímaní sú tvorcovia kódu ako napr. programátori online hry a tvorcovia webových stránok bohmi tvoriacimi pravidlá. Akýsi panteón bohov kódu - tvorcov architektúry kyberpriestoru tvorí tieto pravidlá rôzne a neunifikovane, ktorých znenie potom do značnej miery závisí od ich individuálneho rozhodnutia. Tým nepriamo vynucujú určitý model správania podľa ich pôvodnej predstavy. Tento spôsob môžeme nazvať nepriama regulácia. Tá prezentuje kvalitu informácie vnesenej bohmi kódu, ktorou priamo ovplyvňujú výslednú podobu spoločenského systému. Samotná podstata miery organizácie kyberpriestoru tak závisí i od toho či kód budú tvoriť informácie založené na rozhodnutí represívnych či slobodných tvorcov architektúry¹⁰⁷. Relatívnosť subjektívneho nastavenia tvorcu kódu a jeho decentralizácia v kombinácii s jednoduchosťou prístupu na druhej strane zapríčiňuje vysokú mieru volatility zachovávaní práv, ktorých ochranu užívateľ v kyberpriestore rovnako ako v reálnom priestore legitímne očakáva.

¹⁰⁵ LESSIG, *Code: Version 2.0*, 2006, op.cit., s.83 a násl.

¹⁰⁶ Ako príklad by sme si mohli vziať malé komunity nazvané *guilds* vytvárané v online hrách na hrdinov ako napríklad *World of Warcraft*. V prostredí sa po dobu 14 rokov existencie tejto hry, jej hráči vytvorili na serveroch vlastné dynamické sociálne spoločenstvá nielen k prekonávaniu prekážok nastavených kódom tvorcov online hry, ale k taktiež k socializácii ich virtuálnych avatarov. Interakcia enormnej hráčskej základne sa stala prirodzene ťažiskom mnohých štúdií. napr. epidemiológie: LOFGREN, Eric T. a FEFFERMAN, Nina H.. The untapped potential of virtual game worlds to shed light on real world epidemics. *The Lancet*. 2007, roč. 7, č. 9, s. 625 - 629 ISSN 1474-547X.

¹⁰⁷ ANDRUŠKO, 2016, op.cit., s.34

Kód preberá úlohu práva ako efektívneho regulátora organizovaním ľudského chovania¹⁰⁸ na najnižšej úrovni, ale zároveň pôsobí s ostatnými modalitami vrátane práva v určitej syntéze. V miestach, kde pravidlá uložené kódom prestávajú byť sebestačnými, nastupuje ich suplementácia ostatnými definičnými normami vytvorenými príslušným suverénom napr. štátom alebo súkromným subjektom ako ISP. Vylúčený nie je ani morálny apel spoločnosti. Sieť je tak z ideí neregulovateľného priestoru vytlačená v mene komerčného a morálneho účelu pragmatickými požiadavkami a chovaním jej užívateľov. Potenciálne hrozby zavedenému štandardu ochrany práv však nemôžu byť odvrátené výlučne súkromnými subjektami či spoločnosťou. Túto úlohu preberá štát, ktorý pozitívne stanovuje regulatívny rámec, ktorý obchodu a občanom napomáha chrániť svoj legitímny záujem totožne ako vo vzťahoch v reálnom svete¹⁰⁹. Tento postup je tradičnou priamou reguláciou. Spojením so samoregulačnými tendenciami tvorcov kódu a ostatnými modalitami regulácie sa dostávame k modernému poňatiu metaregulácie.

V globálnej informačnej infraštruktúre vie informácia okamžite a s bezprecedentne nízkymi nákladmi dosiahnuť koncového užívateľa, ktorý sa na jej formovaní ďalej podieľa, ale zároveň chce subjektívne vnímať túto činnosť ako jednak chránenú zákonom ale i liberálne decentralizovanú a anonymnú. Práve pre zachovanie oslobodzujúceho potenciálu tohoto fenoménu, je pre zákonodarcu vhodné zakotviť v právnom poriadku rámec relatívne prudentnej priamej regulácie¹¹⁰. Tá rámcovo stanoví parametre chovania a odpovedajúci sankčný postih. Dospeli sme k poznaniu, že tento spôsob nemôže byť aplikovaný na kyberpriestor výlučne, z povahy regulovaného objektu by nebol efektívny. Trik efektívnej priamej regulácie je aby štát učinil legitímne kroky, napríklad stanovením striktnej hrozby sankcie, ktoré vyvolajú žiadúci vývoj nepriamej regulácie v kyberpriestore, najmä architektúry – kódu. Otázkou ako ju nastavil Lessig, nie je „*ako architektúra Internetu uľahčí*

¹⁰⁸ LESSIG, *Code: Version 2.0*, 2006, op.cit., s.179

¹⁰⁹ LESSIG, *Code: Version 2.0*, 2006, op.cit., s.60 a násl.

¹¹⁰ SAVIN Andrej. *EU Internet Law*. Vyd. 2. Elgar European Law Series, publikované: 28.4.2017 [cit. 25.3.2018]. Dostupné z: www.elgaronline.com/view/9781784717957/10_chapter1.xhtml? s.1

*tradičnú reguláciu, ale ako tradičná regulácia podnieti použitie kódu ako efektívneho regulátora*¹¹¹“.

Z pohľadu legitimacy zvolenej metódy je treba uviesť poznatok tejto práce, že spoločenské vzťahy vznikajúce v rámci informačnej siete i napriek svojej rozdielnej forme, čo do podstaty totožné s tými, ktoré sú štátne právnej regulácii dôverne známe, nie je potreba hľadať a zdôvodňovať nové legitimačné dôvody štátnej regulácie.

2.2.1 Definičné authority

Inšpiráciou Lessigovej teórie regulatívnej sily kódu sa stala vynikajúca práca Joela Reidenberga o povahe riadenia a vytvárania pravidiel v sieti¹¹². V súhrne je jej základnou tézou vytvorenie nového modelu regulácie pre globálnu informačnú sieť postavenej na predpokladoch rozpadu územných hraníc v kyberpriestore a zložitosti vzťahov medzi jeho rôznymi účastníkmi ako štát - vláda, ISP ako prevádzkar informačného systému a poskytovateľ informácií a občan. Obsahovo je Lessigovi prirodzene podobná, obidve vychádzajú z predpokladu, že technické pravidlá globálnej informačnej infraštruktúry sú tvorené tvorcami architektúry a ISP, z ktorých každý vytvára kauzálne pravidlá vo vzťahu k vymedzeným oblastiam infraštruktúry, čím získava atribút držiteľa tradičnej teritoriálnej suverenity¹¹³. Celý tento vzťah je postavený na symbióze interaktívneho fungovania infraštruktúry. Štát má záujem na rozvoji informačnej spoločnosti. Privátny sektor má zásadný význam pri rozvoji globálnej informačnej siete. Technológovia majú kľúčovú pozíciu pri voľbe technických pravidiel siete, ktoré sú sprevádzané rôznymi sociálnymi pravidlami nastavených užívateľmi v kybernetických komunitách. Voľba a nastavenie týchto noriem môže znemožniť alebo podporiť štátne záujmy a ciele občanov¹¹⁴. Všetky tieto subjekty sú teda nadané technickou kompetenciou budovať definičnými normami prostredie

¹¹¹ LESSIG, *Code: Version 2.0*, 2006, op.cit., s.81 a násl.

¹¹² REIDENBERG, Joel R. Governing Networks and Rule-Making in Cyberspace. *Emory Law Journal*. 1996, roč.45, s. 911-930. ISSN 0094-4076

¹¹³ ANDRUŠKO, 2016, op.cit., s.35 a násl.

¹¹⁴ REIDENBERG, 1996, op.cit., s.926

globálnej informačnej siete. Tým súhrnne vytvárajú legitímne regulatívne pravidlá Internetu z pozície definičnej autority¹¹⁵.

2.3 Internetový gatekeeping

O Lessigovom kóde sa dá v prostredí Internetu hovoriť v dvoch úrovniach, jednak ide o základné nastavenie siete, podobné genetickému kódu, ktoré je dané protokolovým štandardom TCP/IP a napríklad identifikáciou a pridelením doménového mena. Táto úroveň je nemenná, ich zmenou by sa celý systém znefunkčnil. Je základom aplikačnej vrstvy, ktorú tvoria internetové prehliadače, operačné systémy, e-mail alebo dátové servery¹¹⁶. Tieto jednotlivé produkty sú vytvárané súkromnými subjektami, najčastejšie ISP a technologickými spoločnosťami. Tieto produkty však často nefungujú samostatne, bez akéhokoľvek následného dohľadu spoločnosti alebo vlastníka webovej platformy. Tým sa určité typy definičných autorít stavajú do pomyselnéj pozície *gatekeepera*¹¹⁷ – strážneho vrátnika informácie na Internetu. V jednoduchšej podstate si takto môžeme prispôbiť staršiu tézu modernému poňatiu úlohy definičnej autority v zmysle ochrany práva prejavu na Internete a nových vyvstávajúcich právnych problémov. Pojem nebudeme definovať priamo v úvode, jeho definíciu si výkladom prispôbíme potrebám práce.

Vymedzenie pojmu *gatekeeper* je medziodborovo nejednotné. Povahu nesúlady najlepšie popísala Barzilai-Nahon¹¹⁸: "*Literatúra o gatekeepingu je fragmentovaná z hľadiska epistemológií, teórií a modelov, slovníkov, heuristiky a výskumných výziev v rámci disciplín a polí a medzi nimi. Stáva sa to preto, lebo diskurz na tému gatekeepingu je vedený v rámci každej disciplíny, v relatívnej izolácii.*"

¹¹⁵ POLČÁK, *Internet a proměny práva*, 2012, op. cit., s. 137

¹¹⁶ LESSIG, *Code: Version 2.0*, 2006, op.cit., s.145 a násl.

¹¹⁷ Budeme používať anglický výraz *gatekeeper*, ako osoby, ktorá je základom procesu filtrovania šírených informácií v spôsobe komunikácie. *Gatekeeper* a *gatekeeping* sú slová zavedené i do slovenského pojmoslovía. Najbližší ekvivalent „vrátnik“ či „strážnik“ sa nejaví ako vhodný.

¹¹⁸ BARZILAI-NAHON, Karine. Gatekeeping: A critical review. *Annual review of Information Science and Technology*. 2009, roč. 43, č.1, s.433-478. ISSN 0066-4200. s.433

Peter Drucker v publikácii Vek diskontuity¹¹⁹ argumentuje, že ľudstvo prešlo z ekonomiky založenej na statkoch na ekonomiku založenú na vedomosti. V ekonomike informačného veku síce stále proklamujeme, že informácie sú zadarmo, ale zároveň žiadna cennejšia komodita ako dobrá informácia neexistuje. História môže potvrdiť skutočnosť, že od doby vzniku konceptu informácie, ubikvitne existovali aj jej strážcovia - *gatekeeperi*, ktorí riadili a kontrolovali šírenie správnych a dobrých informácií. V starovekých civilizáciách napríklad posvätným zvitkom rozumel len veľmi úzky kruh kňazov a mystikov, lebo boli v jazyku, ktorý bol pre väčšinu ľudí nedostupný. V súčasnosti zasa vlády určitých štátov potláčajú správy, ktoré majú potenciál vykresliť ich v negatívnom svetle. Úloha *gatekeepera* môže byť však nie len represívna, ale rovnakou mierou i prospešná. S príchodom internetu žijeme vo veku, v ktorom sú informácie tak ľahko dostupné, že sa môžeme ľahko stať obeťou „preťaženia informáciami“¹²⁰. V tomto novom kybernetickom svete s informáciami je prirodzené, že sa objavili noví *gatekeeperi*, ktorí zohrávajú neoddeliteľnú úlohu v „... procese utvárania a spracovania nespočetných častí informácií do obmedzeného počtu správ, ktoré sa každodenne dostanú k ľuďom“¹²¹. Je jednoduché vidieť paralelu s niektorými definičnými autoritami v kyberpriestore, ich úloha v regulatívnom procese sa tak môže rozšíriť na zabezpečenie dodržiavania ľudských práv a podporu demokratického prostredia na internete prostredníctvom dobre filtrácie šírených správ.

V online prostredí Laidlaw popisuje dve úlohy *gatekeeperov* ako „jedna je nazerat' smerom do vnútra tým, že bráni nejakému správaniu alebo prístupu, a druhá, je nazerat' smerom von, tvarovať správanie alebo vnímanie.“¹²². Ak tento abstrakt prenesieme do prostredia Internetu, nájdeme *gatekeepera* nazerajúceho do vnútra vo forme poskytovateľov internetových služieb - ISP, ktorým bola v niektorých krajinách udelená výsada filtrovať,

¹¹⁹ DRUCKER, Peter F. *The Age of Discontinuity*. Oxford, UK: Butterworth-Heinemann, 1969, 380 s. ISBN 9781483165424

¹²⁰ BAWDEN, David a ROBINSON, Lyn. The dark side of information: overload, anxiety and other paradoxes and pathologies. *Journal of Information Science*. 2009, roč. 35, č.2, s.180-191. ISSN 1741-6485

¹²¹ SHOEMAKER, Pamela J. a VOS, Tim P. *Gatekeeping theory*. New York: Routledge, 2009, . ISBN 0415981395. s.1

¹²² LAIDLAW, 2015, op.cit., s.41

blokovať a odstraňovať určitý obsah spoločensky považovaný za škodlivý.¹²³ Pokiaľ ide o nazeranie von do prostredia, máme na mysli skôr tvarovanie sociálnych noriem. Ideálnym príkladom sú tzv. celebrity sociálnych médií - napríklad veľkí poskytovatelia obsahu do video platformy *YouTube*, ktorí podobne ako celebrity v reálnom svete dokážu vytvárať trendy, či formovať správanie svojich fanúšikov a meniť ich vnímanie sveta. Špecifickým prípadom sú internetové vyhľadávače, napríklad najznámejší *Google*, ktorý je schopný nasmerovať používateľov k špecifickým informáciám založeným na kritériách optimalizácie vyhľadávania alebo informáciách o preferenciách používateľov, ktoré vyhľadávače získali skrytým sledovaním užívateľskej aktivity. Existuje napríklad len veľmi málo užívateľov Internetu, ktorí by niekedy vyhľadávali informácie až na štvrtej stránke výsledkov vyhľadávania internetových vyhľadávačov, a teda môžeme tvrdiť, že majú vo výsledku relatívne podobný účinok ako blokovanie alebo skrytie určitých informácií.

Pre porozumenie úlohy *gatekeepera* na Internete krátko odkážeme na Barzilai-Nahonovej *Network Gatekeeper Theory* (Teóriu gatekeeperov siete, pozn.), ktorou aplikovala svoje poznatky osobitne na prostredie siete internetu, teda od tradičného poňatia procesu šírenia informácií do poňatia kontroly informácie¹²⁴. Využívajúc tento rámec odôvodňujeme potrebu *gatekeeperov* pri vytváraní demokratického prostredia internetu, v ktorom sa dodržiavajú ľudské práva. Laidlaw odlišuje dvoch základných aktérov tejto teórie ako *gatekeepera* a *internetového informačného gatekeepera* (Internet information gatekeeper – IIG, pozn.)¹²⁵.

2.3.1 Rámec Network Gatekeeper Theory¹²⁶

Barzilai-Nahon, definuje tradičný *gatekeeping* ako „proces riadenia informácií pri prechode cez bránu. Činnosti sieťového *gatekeepingu* zahŕňajú výber, pridanie, zadržanie,

¹²³ Bližšie v kapitole 4.2 a násl.

¹²⁴ BARZILAI-NAHON, Karine. *Toward a Theory of Network Gatekeeping: A Framework for exploring information control* [online]. Network Gatekeeper, publikované 12/2007 [cit. 10.4.2018]. Dostupné z: ekarine.org/wp-admin/pub/GatekeepingSalienceTheory.pdf

¹²⁵ LAIDLAW, 2015, op.cit., s.44 - 56

¹²⁶ Network Gatekeeping Framework, pozn.

zobrazenie, smerovanie, tvarovanie, manipulácia, opakovanie, načasovanie, lokalizácia, integrácia, ignorovanie a vymazanie informácií.“ Gatekeeperi v zmysle rámca *Network Gatekeeping Theory* sú rozdelení do podobných kategórií ako definičné authority:

- a) Formálny regulátor - medzinárodná organizácia, alebo štát,
- b) Regulátor infraštruktúry - verejné alebo súkromné orgány, ktoré majú právomoc regulovať správanie používateľov v súvislosti s infraštruktúrou,
- c) Poskytovateľ služieb, ktorí poskytujú platformu digitálnej seberealizácie virtuálnej komunity a slúžia ako subjekt, ktorý zastupuje komunitu externe vo vzťahu k formálnym regulátorom.
- d) komunitných manažérov, ktorí majú zodpovednosť za každodennú prevádzku svojich komunit, a
- e) členov virtuálnej komunity, ako individuálnych užívateľov ale aj jej reprezentantov.

2.3.1.1 Internetoví informační gatekeeperi

Laidlaw zdôrazňuje, kedy sa obchodná spoločnosť vyvíja tak, že je iba tradičným gatekeeperom, a preberá úlohy *internetového informačného gatekeepera – IIG*. V prípade, že menšie webové stránky alebo platformy majú schopnosť pôsobiť ako gatekeeperi prostredníctvom riadenia toku informácií na svojich webových stránkach, nie sú nevyhnutne IIG. "*Práve vtedy, keď sa priestor, ktorý spravujú, stáva priestorom, ktorý uľahčuje alebo bráni demokratickému prejavu, subjekt gatekeepera participuje na demokratickej kultúre.*" Z tohto dôvodu sa iba *gatekeeper*, ktorá uľahčuje alebo bráni účasti na demokratickej kultúre, považuje za IIG. To je podľa Laidlaw forma základnej spoločenskej zodpovednosti podnikov (corporate social responsibility – CSR, pozn.), v ktorej obchodné spoločnosti „*zodpovedajú za ľudské práva v rámci svojej sféry vplyvu*“¹²⁷. Laidlaw načrtáva dopad jednotlivých činností v modeli IIG na právny demokratický systém na základe ich povinností v oblasti zachovávania ľudských práv. Určité IIG musia internetoví používatelia k prístupu a navigácii na internete použiť takmer bezpodmienečne (napr. poskytovatelia internetového pripojenia

¹²⁷ LAIDLAW, 2015, op.cit., s.47

a internetové vyhľadávače, pozn.), tie majú tradične primárnu úlohu *gatekeepingu* v oblasti ľudských práv, preto ich nazývame aj „*macro - gatekeeper*“. Ďalšie úrovne IIG, ktoré nie sú pre internetovú skúsenosť užívateľa nevyhnutné (veľké sociálne a mediálne platformy ako Facebook, Youtube a pod., pozn.) sú až druhotnými autoritami „*micro - gatekeepermi*“, pretože kontrolujú iba predom vymedzený určitý obsah na základnej úrovni.

Ako sa kybernetický priestor rozširuje a čoraz viac je ľudský prejav prenášaný do online platformy (blogy, platformy sociálnych médií), konečná sila, ktorá technicky rozhoduje o praktickom výkone tohto práva, leží v rukách gatekeeperských gigantov, ako sú Google, Facebook, Youtube, AOL a pod. Zdá sa však, že platforma slobodného prejavu s potenciálom osloviť celosvetové publikum je ohrozená kvôli nedostatku globálneho zamerania na to, ako je prejav v tejto platforme skutočne regulovaný.

Reidenberg (2004) vysvetľuje¹²⁸, že „*Rovnako ako sa pravdepodobne sa postupne prejaví právna zodpovednosť voči poskytovateľom [ISP], poskytovatelia sa stávajú čoraz atraktívnejšími ako entity presadzovania pravidiel. Pokušenie používať poskytovateľov pochádza zo sútoky dvoch faktorov. V rozsahu, v akom sú početní a rozptýlení skutoční delikventi, bude štát potrebovať značné zdroje na to, aby sa vyhrážal každému delikventovi osobitne, a naviac sa takéto prenasledovanie pravdepodobne stretne s praktickými prekážkami. Naopak, v miere v ktorej sú aktivity rozptýlených delikventov smerované cez prístupové brány [služieb ISP], je ich možné prostredníctvom poskytovateľov ľahšie dosiahnuť a ponúknuť efektívnejšie výsledky. Centralizácia činnosti prostredníctvom prístupových brán poskytuje štátnym orgánom nové možnosti presadzovania práva.*“

Z tohto pohľadu je zrejmé, že úloha ISP v roli IIG je podľa tejto teórie uľahčiť udržanie štandardu základných ľudských práv v obrovskej šírke kybernetického priestoru. Takýto postup by mal byť samozrejmosťou, pretože formálny regulátor nemá rovnaký dosah ani pracovnú silu na riadenie expanzívneho globálneho prostredia a túto úlohu nepriamo deleguje. Z povahy decentralizovaný internet je odzrkadlený aj decentralizovaným regulačným mechanizmom, kde neexistuje centrálny národný ani globálny regulačný orgán,

¹²⁸ REIDENBERG, Joel R. States and Internet Enforcement. *University of Ottawa Law & Technology Journal*. 2003, roč. 1, č. 1-2, s. 213-230. ISSN 1710-6028. s.224

ktorý by centrálnne vynucoval dodržiavanie práva v tomto prostredí. V súčasnosti existuje hybridná forma regulácie, ktorá leží niekde medzi meta a samoreguláciou z hľadiska postupov v oblasti *gatekeepingu* a je nevyhnutné, aby v záujme adekvátneho dodržiavania ľudských práv a demokracie na internete formálny regulátor zohrával väčšiu úlohu pri nastavení parametrov toho, čo je v súčasnosti samoregulované.

K lepšiemu pochopeniu konceptu uvedieme krátky príklad úlohy *gatekeeperov* v regulačnom rámci, kde môže byť kybernetický priestor prirovnávaný k mestu nazvanému Cyberspace. Prvým *gatekeeperom*, s ktorým by sme sa stretli pri cestovaní do mesta, by bol strážnik brány menom ISP, ktoré podľa modelu IIG predstavuje *macro-gatekeepera*. Blokovanie prístupu k obsahu poskytovateľmi služieb informačnej spoločnosti sa môže prejaviť v prípadoch, keď sú zablokované nelegálne stránky hazardných hier, a to rovnakým spôsobom, ako by bolo kasíno bez príslušnej licencie pre obyvateľov mesta Cyberspace uzatvorené.

V meste sa nachádzajú rôzne inštitúcie, ako sú napríklad knižnice, reštaurácie a univerzity [*platformy sociálnych médií, on-line diskusné fóra, blogy, internetové vysielanie a hranie hier*], ktoré sa riadia právnym rámcom a na jeho základe dobrovoľne implementujú svoje vlastné samoregulácie vo forme činnosti *gatekeepingu*. Občania, ktorí navštevujú konkrétne destinácie sa podriaďujú vlastným pravidlám správania a prístupu každej lokality. Ak napríklad chcete navštíviť univerzitnú knižnicu, potrebujete prístupovú kartu s identifikačnou fotografiou, aby ste sa dostali za turnikety [*online knižnice, ktoré vyžadujú používateľské mená, prihlasovacie informácie a overenie e-mailom*]. Webové stránky, platformy a aplikácie sociálnych médií by podľa modelu IIG boli zaradené do kategórie *micro-gatekeepers* v závislosti od ich dosahu a skutočného vplyvu na kultúru a práva na slobodu prejavu. V ich prípade platí, že čím menší majú dosah, tým menej vedia ovplyvniť právo. Keď občania vstúpia na uvedené miesta, od verejných námestí, stretnutí radnice až po prednášky, možnosti ich angažovanosti sa líšia a sú určené inštitúciou. Občania by mohli byť vyradení zo zariadení kvôli neetickému správaniu sa alebo nedodržiavaniu sociálnych noriem takýchto miest. Občan by mohol byť ako príklad zatknutý za verejnú nahotu alebo by občania mohli byť vyradení z verejného fóra za rasistické pripomienky. Diskusné fóra internetových stránok sú schopné zablokovat' poskytovateľov obsahu a koncových užívateľov, ktorí

vnášajú rasistické poznámky alebo zdieľajú pornografický materiál. Platforma, akou je napríklad Youtube, by sa považovala za autoritatívneho gatekeepera a mala väčšiu zodpovednosť za to, aby zabezpečila dodržiavanie ľudských práv vďaka svojej enormnej pôsobnosti a dosahu; zatiaľ čo malý osobný blog s postavením s primeraným rozmerom by sa považoval za *micro-gatekeepera*.

K dôsledkom veľmi zaujímavej *Network Gatekeeping Theory* celistvo odkážeme na práce Laidlaw a Barzilai-Nahon, avšak v našom ponímaní bude zohrávať v budúcnosti regulácie internetových sietí čoraz výraznejšiu úlohu. V súčasnosti je skôr na dobrovoľnej aplikačnej úrovni, ktorú na seba prevziali v rámci zodpovednosti spoločnosti a veľké internetové komunity a je možno najvyšší čas dodať týmto definičným normám výraznejší normatívny rámec zákonom.

2.3.2 Voľne k problémom internetovej regulácie

Zrkadlenie spleťového charakteru internetu je jeho rovnako zložitý prepojenie s regulačnými pravidlami. Feick a Werle¹²⁹ opisujú túto realitu ako stretnutie s "*čiasťovo komplementárnymi, čiastkovo konkurenčnými regulačnými prvkami vo forme právnych predpisov a nariadení, povinných a dobrovoľných technických noriem a protokolov, medzinárodných a národných zmlúv a dohôd a neformálnych kódexu správania a net etikety*". S cieľom vytvoriť štruktúru v rámci tohto pandemónu regulačných prvkov rozdeľujeme nariadenie na dve skupiny:

1. Prístup k infraštruktúre: zameranie sa na rozvoj organizovaného spôsobu zabezpečenia technických noriem, poskytovateľov pripojenia pri prenose obsahu
2. Prístup k obsahu: regulácia samotných činností, ktoré sa týkajú výlučne internetového prostredia a nemožno ich analogicky prenášať do reálneho sveta

Bez ohľadu na právny rámec, obsah na internete si vyžaduje reguláciu a zváženie nielen z hľadiska právnej bezpečnosti, ale aj morálnej ochrany. Samotná cenzúra teda neovplyvňuje iba šírenie revolučných a protištátnych myšlienok v autoritatívnych režimoch, ale aj obsah, ktorý by mal byť vnímaný ako škodlivý v morálnej spoločnosti, a cenzúra by sa

¹²⁹ BALDWIN, CAVE a LODGE ed., 2010, op.cit., s.525

mala javiť ako jednostranné východisko postoja štátov pri pokuse obmedziť prístup detí a dospelých k informáciám a materiálom s negatívnym dopadom na ich zdravý morálny a sociálny rozvoj. Do tejto kategórie patrí narastajúci počet xenofóbnych a extrémistických stránok, stránky s otvorene sexuálnym obsahom a stránky ponúkajúce prístup k nelicencovaným hazardným hrám. Podkategóriou, ktorá nebude v tejto práci, je regulácia pre ktorú internet pôsobí len ako ďalšie špeciálne médium, priestor pomocou ktorého sa uzatvárajú zmluvy alebo porušujú autorské práva.

3 Právna zodpovednosť pri používaní internetu

Pri vymedzení kyberpriestoru v predchádzajúcej časti sme naznačili, že v súčasných celospoločenských podmienkach nemôže byť považovaný za priestor vyňatý z pôsobnosti právnych noriem, ktoré dopadajú na jeho jednotlivé subjekty v reálnom svete. Taktiež sme dospeli k poznaniu, že autoritatívna regulácia nepredstavuje jedinečný prístup k systematickej organizácii prenášania informácií, ktorá je v dominantnej miere samoregulovaná¹³⁰. Jej hlavným prínosom, je však zamedzenie roztrieštenia komplexného prirodzene právneho modelu mnoho stupňovej organizácie, kde na úrovni autority pôsobí štát a verejná správa, ktorým sa podriaďujú jej jednotlivé subjekty v sieti - užívatelia a recipienti (ISP, koncový užívateľ, pozn.). Pre úplnosť pochopenia právne pozitívneho východiska regulácie objektu, nemôžeme opomenúť dôležitú otázku vzniku a realizácie právnej zodpovednosti niektorých definičných autorít.

Krátkym exkurzom do pochopenia *zodpovednosti* v česko-právnych reáliách rozpoznávame štruktúru pojmu na viacerých úrovniach, z ktorých priblížime spoločenský základ právnej zodpovednosti ako základnej formy realizácie práva¹³¹. Samotnú koncepciu zodpovednosti v českom práve ako základného právneho pojmu následne aplikujeme na prostredie internetu a okruh konkrétnych subjektov, na ktoré dopadá. Teoretický pojem právnej zodpovednosti koncipujeme ako formu právneho vzťahu, ktorý vzniká na základe porušenia existujúcej primárnej právnej povinnosti ku vzniku a uplatneniu nepriaznivých právnych následkov voči subjektom, ktoré právnú povinnosť porušili¹³².

Osobitnú podmnožinu tvorí správnoprávna zodpovednosť tj. za priestupky, pre ktorú je charakteristické protiprávne jednanie subjektov práva, za ktoré je možné uložiť správnoprávnu sankciu, ktorá je realizovaná správnymi orgánmi¹³³. Ako uvádza Průcha,

¹³⁰ Tomuto prístupu môže chýbať na najnižšej úrovni užívateľa definičný znak autority. Myšlienkový prístup prevzatý z POLČÁK, *Internet a proměny práva*, 2012, op. cit., s.88 a násl.

¹³¹ GERLOCH, Aleš. *Teorie práva*. 3. rozš. vyd. Plzeň: Aleš Čeněk, 2004, 343 s. Právnické učebnice (Aleš Čeněk). ISBN 8086473856. s.178

¹³² *ibid* s.179 a násl.

¹³³ PRŮCHA, Petr. K pojetí správněprávní odpovědnosti a správního trestání. *Správní právo*. Praha: Ministerstvo vnitra. 2014, roč. 2014, č.1-2, s. 16-27. ISSN 0139-6005 s.16

takéto poňatie správnej zodpovednosti je prejavom sankčnej koncepcie retrospektívneho chápania právnej zodpovednosti, podľa ktorej zodpovednosť vzniká a nastupuje až v dôsledku porušenia primárnej právnej povinnosti a jej uplatnenie sa prejavuje v uložení sankcie. V tomto zmysle je uvedená koncepcia protipólom tzv. aktívneho chápania právnej zodpovednosti, ktoré kladie vznik zodpovednosti do okamihu vzniku primárnej právnej povinnosti, tzn. do skoršieho štádia, než táto povinnosť mohla byť porušená¹³⁴.

Vo verejnej správe sa jadro princípu zodpovednosti *neminem laedere* presadzuje osobitne tak ako je uznávaná potreba existencie správneho práva¹³⁵. Potenciálne zodpovedný subjekt volí svoje vnútorné nastavenie v rámci normality a rozhoduje sa pre zodpovedné a nezodpovedné chovanie. V pojmovej konštrukcii verejnoprávnej zodpovednosti nájdeme však i príčinnú (kauzálnu) zodpovednosť a sekundárnu povinnosť odškodnenia resp. nápravy. Vznik škody je na voľbe činnosti subjektu neporušiť žiadnu primárnu povinnosť nezávislý, avšak aj tak je v priamej príčinnej súvislosti s jej vznikom¹³⁶.

V zložitej štruktúre zodpovednostných vzťahov na internete nie je verejnoprávna zodpovednosť jedinou a ani ťažiskovou. Tou sa z povahy objektu stáva súkromnoprávna povinnosť nahradiť škodu, ktorá sa uplatní napríklad vo vzájomnom vzťahu ISP a koncových užívateľov alebo koncových užívateľov vzájomne pri porušení autorských práv alebo zmluvy.

Iným základným rozdelením je zodpovednosť subjektívna, pri ktorej sa zohľadňuje miera zavinenia ako vnútorného psychického vzťahu subjektu k jednaniu a následku a ich stupňovej modality a zodpovednosť objektívna. Pri druhom type zodpovednosti nie je vyžadovaný vnútorný vzťah k protiprávnosti jednania, ktorú teda adekvátne konštruujeme ako zodpovednosť za výsledok, pre ktorej vznik nie je zavinenie predpokladom. Hovoríme o nej ako o výsledku nezavineného protiprávneho jednania. Obvykle je dopad striktnej zodpovednosti zmierňovaný možnosťou liberácie predstavujúcej zákonne definované

¹³⁴ *Ibid* s.20 a násl.

¹³⁵ POMAHÁČ Richard et al. *Veřejná správa*. 1. vyd. Praha: C.H.Beck, 2013, 315 s. ISBN 9788074004476. s.159

¹³⁶ *ibid*, s.160

podmienky pri preukázaní ktorých, sa inak zodpovedný subjekt môže tejto zodpovednosti oprostiť. Práve takéto právne teoretické poňatie vzniku novej sekundárnej povinnosti sankčného charakteru je základom zodpovednosti poskytovateľov služieb informačnej spoločnosti v českom a európskom práve.

3.1 Doktrínálne východiská poskytovania služieb informačnej spoločnosti

Pri prenose inštitútu deliktuálnej zodpovednosti do kyberpriestoru neopúšťame priestor pozitívneho práva, ktoré sa prípadne *per analogiam* uplatní rovnako pre delikty v reálnom svete. Môžeme tvrdiť, že naopak povinnosťou štátu ako regulátora nadaného mocou, je právne pravidlá odvodzovať, vytvárať a vynucovať už len na základe samotnej univerzality práva, a to i na spoločenské vzťahy, ktoré by svojou rozdielnosťou formy mohli ľahko uniknúť vecnej pôsobnosti právnych noriem¹³⁷. Povaha týchto vzťahov však prináša do základných princípov nové otázky, napríklad vymedzenia pôsobnosti, práva na súkromie a slobody prejavu na ktoré treba nepochybne vzťahnúť i princíp legitímneho očakávania subjektov ochrany týchto práv v novom prostredí, a to i za cenu oslobodenia výkladu od konzervatívneho významového chápania a aplikácie.

Virtuálne delikty od reálnych odlišuje najmä supraterritoriálny a anonymný charakter internetu v kombinácii so zvláštnou povahou vzťahov, ktoré na ňom vznikajú¹³⁸. Ako ďalej Lukáš Vondřích poznamenáva, v architektúre fungovania internetu majú poskytovatelia internetového pripojenia výsadné postavenie ako jediné subjekty technicky schopné filtrovať nielen požiadavky koncových užívateľov, ale i zobrazovaný obsah v ponúkanej platforme. Samotný digitálny obsah svojou kvantitou núti zákonodarcu opustiť tradičné hranice dohľadu. Inými slovami, pri zakotvovaní ustanovení o zodpovednosti nemôže zákonodarca pozitívne predpokladať kladné prijatie akejkoľvek argumentácie stáleho monitoringu služieb internetu jeho poskytovateľmi. Na tomto obsahu sa podieľa tvorbou najmä koncový užívateľ

¹³⁷ POLČÁK, *Internet a proměny práva*, 2012, op. cit., s.97 a násl.

¹³⁸ VONDŘICH, Lukáš. *Mezinárodně-právní aspekty deliktů odpovědnosti na internetu* [online]. Disertační práce. Univerzita Karlova v Praze, Právnická fakulta. Vedúci práce Monika Pauknerová. 2016, s. 54 [cit. 23.3.2018]. Dostupné z: <https://is.cuni.cz/webapps/zzp/detail/146874/>

svojou aktivitou. Pri pojednávaní o verejnoprávnej ochrane globalizovaných informačných štruktúr a stanovení právnej regulácie internetu nám vyvstávajú primárne otázky miery (ne)zodpovednosti poskytovateľov služieb informačnej spoločnosti za zverejňovaný obsah a šírenie informácií užívateľmi.

Základným východiskom sa stala limitácia právnej zodpovednosti poskytovateľov služieb informačnej spoločnosti v súvislosti so zaisťovaním a poskytovaním služieb v prostredí internetu dynamickému okruhu užívateľov v spojení s neexistenciou všeobecnej povinnosti dohľadu. Pri aplikácii všeobecných ustanovení o príslušnej zodpovednosti, by poskytovatelia nemohli operovať bez limitácie užívateľského prístupu a zavedenia inštrumentálnych prevenčných opatrení, ktoré by však v súhrne podnietili vysoké administratívne náklady pretavené v užívateľské poplatky, čím by sa stal internet akousi exotickou platformou majetnej vrstvy v spoločnosti. V opačnom prípade by vznikala hrozba neprimeranej sankcie v situáciách, ktorým nie je možné adekvátne, zo strany poskytovateľa predchádzať.

Miera v ktorej zodpovednosť preberajú nielen subjekty zverejňujúce alebo šíriace prostredníctvom internetu určitý obsah, ale taktiež poskytovatelia služieb informačnej spoločnosti – platforiem na digitálnu sebarealizáciu je preto upravená špeciálnym zákonom č. 480/2004 Sb. , o niektorých službách informačnej spoločnosti a o zmene niektorých zákonů, ktorý implementuje dve smernice EÚ do českého právneho poriadku, a to konkrétne smernice Európskeho parlamentu a Rady č. 2000/31/ES¹³⁹ a smernice Európskeho parlamentu a Rady č. 2002/58/ES¹⁴⁰. Výkladové ustanovenie §2 ZoNSIS sa zaoberá najmä definovaním niektorých esenciálnych pojmov, z ktorých po krátkom exkurze do problematiky rozdielnosti poňatia *obsahu* v kapitole 3.2 postupne predstavíme: (a) službu informačnej spoločnosti, (b) poskytovateľa týchto služieb, (c) užívateľa, a sprievodné pojmy.

¹³⁹ Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode), smernica o e-obchode

¹⁴⁰ Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovania osobných údajov a o ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách)

Pre doplnenie právne historického kontextu uvádzame, že do doby adaptácie smernice o e-obchode bola úprava zodpovednosti subjektov na internete za cudzí a vlastný obsah ponechaná prevažne na aplikácii nešpecializovaných právnych noriem od ktorých sa pre potreby vydania rozhodnutia odvádzalo v individuálne určených prípadoch *per analogiam* predmetu úpravy.

V súlade so smernicou o súkromí a elektronických komunikáciach sa jej ciele zákonom spracovávajú i v odvetví správneho práva, v ktorých sa ZoNSIS venuje podmienkam šírenia obchodných zdení¹⁴¹ elektronickým prostriedkami, udeleniu a možnostiam revokácie súhlasu adresáta. Rovnako sa venuje aj právnej zodpovednosti šíriteľov nevyžiadanej elektronickej pošty, ktorá nespĺňa podmienky riadneho označenia, skrýva totožnosť odosielateľa alebo je zaslaná bez platnej adresy, pomocou ktorej môže adresát zamedziť ďalšiemu zasielaniu. ZoNSIS ustanovuje Úrad pre ochranu osobných údajov ČR ako orgán dozoru nad dodržiavaním v časti nevyžiadaných obchodných zdení, ktorý však z dikcie zákona nad oblasťou zodpovednosti ISP dohľad nevykonáva. ZoNSIS sankcie kategorizuje v §11 vo forme priestupkov a v §13 je vymedzený vo vzťahu k zákonu č. 500/2004 Sb., správni rád ako špeciálny, teda SŘ sa použije subsidiárne.

3.2 Krátko ku rozdielu prenosu a šírenia obsahu

V prechode ku globálnej informačnej spoločnosti sa prudkým nárastom možností využitia nových technológií, ktoré sa stali základom takmer každej sektorovej ekonomiky stalo efektívne ukotvenie regulovaného trhu elektronických komunikácií. Termín elektronická komunikácia je konvergenciou nielen výrazových termínov telekomunikácií, mediálnych a informačných technológií ale tiež sprievodným javom rozvoja týchto sektorov. Službami elektronických komunikácií s odvolaním sa na čl. 2 c) smernice č. 2002/21/ES¹⁴²

¹⁴¹ Výkladové ustanovenie § 2 písm. f) ZoNSIS: „Obchodním sdělením všechny formy sdělení, včetně reklamy a vybízení k návštěvě internetových stránek, určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku osoby, která je podnikatelem³ nebo vykonává regulovanou činnost“.

Za takéto zdielanie považujeme taktiež reklamu podľa zvláštneho právneho predpisu.

¹⁴² Smernica Európskeho Parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica)

sú služby poskytované „úplne alebo prevažne z prenosu signálov v elektronických komunikačných sieťach“, vrátane telekomunikačných alebo vysielacích sietí. Výraz však vylučuje služby riadiace obsah a služby informačnej spoločnosti, ktoré nezahŕňajú prenos signálu. V tejto súvislosti treba zmieniť oddelenie regulácie obsahu a sprievodnej zodpovednosti za šírený a prenášaný obsah a regulácie prenosu, ktorá je primárne upravená zákonom č. 127/2005 Sb., o elektronických komunikáciách. Zákon o ElKom je typickým *lex specialis* správnoprávnej regulácie stanovenia podmienok podnikania a výkonu štátnej správy, vrátane regulácie trhu v tejto oblasti¹⁴³. Ťažiskovou úpravou je definovaná právomoc, postavenie a vnútorná štruktúra Českého Telekomunikačního Úřadu, ktorý pôsobí ako správny orgán vytvárajúci podmienky pre podnikanie v komunikačných činnostiach, pod ktorými rozumieme zaisťovanie siete elektronických komunikácií a poskytovanie služieb elektronických komunikácií¹⁴⁴.

I pri existencii zásady oddelenia obsahu a prenosu je pre potreby ďalšieho výkladu v centrálnych častiach 3 a 3 nutné rozlíšiť medzi¹⁴⁵:

- a) obsahom ako *prenášanou informáciou* prostredníctvom siete elektronických komunikácií (ZoElKom), a
- b) obsahom, ktorý niekto *vytvára a šíri* prostredníctvom siete elektronických komunikácií ku koncovému užívateľovi (ZoNSIS).

Sieť elektronických komunikácií druh prenášanej informácie - obsahu zásadne nerozlišuje¹⁴⁶, čo zodpovedá i európskym požiadavkám sieťovej neutrality. Základom regulácie je uplatnenie rovnakých regulačných pravidiel voči všetkým druhom siete, teda i internetu a služieb elektronických komunikácií ako napríklad vysielania. Pri oddelení obsahu môžeme hovoriť o oddelení regulátorov prenosu – ČTÚ, a obsahu vysielania – Rada pre rozhlasové a televízne vysielanie ČR, tá ale z náplne vlastnej činnosti a pravidiel prístup

¹⁴³ VANÍČEK, Zdeněk, MATES, Pavel a NIELSEN, Tomáš. *Zákon o elektronických komunikáciách. Komentář*. Praha: Linde Praha a.s., 2014, 560s. ISBN 9788072019441. s.34 a násl.

¹⁴⁴ Srov. §§ 1; 5 odst. 3) a 7 odst. 1) Zákona o ElKom

¹⁴⁵ Rozdelenie podľa VANÍČEK, MATES, NIELSEN, 2014, op.cit., s.44

¹⁴⁶ §2 písm. h) Zákona o ElKom

k obsahu na internete v prevažnej miere nereguluje. Práve preto sa následne pozrieme na výber možností regulovania internetového obsahu a spôsob konverencie verejnoprávnych a súkromnoprávnych predpisov s možnosťami prijatých opatrení na úrovni poskytovateľa služieb elektronických komunikácií, s dôrazom na internetovú sieť. V zásade k tejto problematike uvádzame, že ani v prostredí internetu nie je striktné oddelenie prenosu a obsahu možné. Obidva sektory sú previazané. Bez prístupu k sieti nemôže byť obsah zobrazený a prijatie opatrenia poskytovateľa môže vyústiť v blokáciu určitého obsahu.

3.2.1 Informačná spoločnosť

V prípadoch abstraktných pojmov, akým je zaiste i *poskytovanie služieb informačnej spoločnosti* musíme opustiť tradičné sémantické uchopenie a strategicky zdôrazniť jednotlivé aspekty pojmu. Až odôvodnením chápania krátkych definícií jednotlivých aspektov znalosťami, sa dostaneme k organizovanému výkladu tohoto fenoménu.

Pri informačnej spoločnosti s určitou formou rečnickej hyperboly, môžeme polemizovať o troch vlnách technologickej revolúcie, ktoré boli začiatkom epoch rekonštitúcií sociálneho sveta: poľnohospodárska, priemyselná a informačná revolúcia. Poukážeme aspoň napríklad na dielo a často citovaný výrok Nasbitta: „*Technológia počítaču je pre informačný vek podobného významu ako predstavovala mechanizácia pre industriálnu revolúciu*“¹⁴⁷. Na obrate milénia sa vďaka masovému šíreniu technológie stal pojem informačná spoločnosť rozšíreným označením pre nové usporiadanie spoločnosti ako uvádza Murányi¹⁴⁸, v ktorom efektívna globalizácia informačných a telekomunikačných technológií umožňuje ľuďstvu viesť nový typ života, mať vyššiu životnú úroveň, lepšiu prácu a úlohu v spoločnosti. Charakteristickým prínosom globálnej informačnej štruktúry je prepojenie všetkých oblastí ekonomiky a sociálneho života v korelácii s informačnou politikou štátu, ktorá zvýšila možnosť rýchleho prístupu neobmedzeného užívateľského okruhu k množstvu

¹⁴⁷ NASBITT, John. *Megatrends: Ten New Directions Transforming Our Lives*. Vyd. 1. New York: Warner Books, 1982, 290s. ISBN 978-0446512510. s.22

¹⁴⁸ Vlastný preklad autora výroku Murányi Béla k informačnej spoločnosti - *információs tarsadalom*. [cit. 24.3.2018]. Dostupné z: <http://comm-media.com/hu/abc/informacios-tarsadalom>

verejných informácií. Pojem informačná spoločnosť uvádza anglický sociológ Webster v obecnej kvantitatívnej a kvalitatívnej perspektíve¹⁴⁹, ktoré vzájomne podmieňuje - príčinu vzniku nového druhu kvalitatívnej spoločnosti kauzalitou kvantitatívnej zmeny v informáciách¹⁵⁰. Kvantitatívne poňatie je zamerané predovšetkým na technickú dostupnosť infraštruktúry prostriedkov k tvorbe, šíreniu a dostupnosti informácií, ktorými jedinci v spoločnosti komunikujú navzájom a zároveň sú spojení s dostupnými autoritami. Krátko si pod týmto spomeňme na predstavenú tézu viacvrstvovej vertikálnej štruktúry regulácie internetu v ktorej sa jednotlivé autority a recipienti podieľajú na súhrne regulácie v informačnej spoločnosti. Horizont takej štruktúry by pritom zdôrazňoval kvalitatívne hľadisko šírených informácií vo vertikálnej osi. Informačnou spoločnosťou by vo výsledku bolo spoločenstvo využívajúce všetky stupne horizontality k necenzúrovanému šíreniu a prijímaniu informácií vysokej kvality¹⁵¹.

Je nepopierateľné, že popri obchodnom sektore i štátny sektor alokuje na informačnú politiku väčšiu pracovnú kapacitu a priradzuje markantnú dôležitosť jej rozvoju¹⁵², čím sa následne z pozície autority vytvára predpoklad zlepšenia celkovej kvality života jednotlivých občanov, ako aj zefektívnenie štátnej správy, samosprávy a podpory rozvoja podnikania v informačnej spoločnosti.

3.2.2 Služba informačnej spoločnosti

Pre pochopenie právneho pojmu *služba informačnej spoločnosti*, rozoberieme príslušné výkladové ustanovenie ZoNSIS v spojení s adaptovanou smernicou o e-obchode. Pre prípadnú realizáciu zodpovednosti za (vlastný a) cudzí obsah pri poskytovaní služieb

¹⁴⁹ WEBSTER, Frank. *Theories of the Information Society*. 3. vyd. New York: Routledge, 2006, 323 s. ISBN 0203962826. s.21

¹⁵⁰ *ibid.*, s.9

¹⁵¹ BOYLE, J. *Shamans, Software, and Spleens: Law and the Construction of the Information Society*. Cambridge, MA: Harvard University Press, 1997, 288s. ISBN 0674805224. s.1 a násl. a s.29

¹⁵² POLČÁK, *Internet a proměny práva*, 2012, op.cit., s.276. S poskytovaním služieb informačnej spoločnosti štátom sa vžil termín e-Government ako cesta posilnenia funkcie dostupnosti verejnej správy v informačnej spoločnosti.

informačnej spoločnosti ich poskytovateľom (Information Service Provider - ISP, pozn.) ako definičnej autority je ťažiskom práve táto zákonná definícia. ISP má výlučnú technickú právomoc zamedzenia prístupu k obsahu, ktorým sa porušujú určité právne normy napr. autorského práva¹⁵³.

Pojem *služba informačnej spoločnosti*, ktorého právny obsah budeme ďalej analyzovať je definovaný v §2 písm. a) v zákone č. 480/2004 Sb. ako: „*jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu; služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat*“.;

Z dikcie ZoNSIS sa javí náročným porozumieť podstate jednotlivých prvkov pojmu, bez ich príslušnej konkretizácie s výnimkou pojmu *poskytovanie elektronickými prostriedkami*. V prípade legislatívneho opomenutia vysvetlením definičných znakov nazrieme v analýze do východiskovej legislatívy - smernice o e-obchode v čl. 2 písm. a), ktorá si znenie definície vypožičiava v zmysle článku 1 odst. 2 smernice č. 98/34/ES, naposledy zmenenej a doplnenej smernicou č. 98/48/ES o postupu pri poskytovaní informácií v oblasti noriem a technických predpisov¹⁵⁴. K uplatneniu technickej definície nám slúži i recitál č. 18 smernice o e-obchode, ktorý vymedzuje príkladný rozsah hospodárskych

¹⁵³ ANDRUŠKO, 2016, op.cit., s.94

¹⁵⁴ „*Služba*“ je každá služba poskytovaná informačnou spoločnosťou, to jest každá služba, ktorá sa bežne poskytuje za odmenu, na diaľku, elektronickým spôsobom a na základe individuálnej žiadosti príjemcu služieb. Na účely tejto definície:

- „*na diaľku*“ znamená, že služba sa poskytuje bez toho, aby pri tom boli obe strany súčasne prítomné,
- „*služba poskytovaná elektronicky*“ znamená, že služba sa z miesta pôvodu odošle a na mieste určenia prijíma prostredníctvom elektronického zariadenia, určeného na spracovávanie (vrátane digitálneho komprimovania) a uskladňovanie údajov a je úplne vysielaná, prenášaná a prijímaná po drôte, prostredníctvom rádiových vĺn, optickým spôsobom, alebo inými elektromagnetickými prostriedkami,
- „*na základe individuálnej žiadosti príjemcu služieb*“ znamená, že služba sa prostredníctvom prenosu údajov poskytuje na individuálnu žiadosť.

činností online, ktoré možno považovať za službu informačnej spoločnosti v troch dimenziách:

- a) služby v poskytovaní nákupnej platformy, pre uzatvorenie kúpnej zmluvy ako napr. online predaj tovaru;
- b) služby, ktoré nehradia jej príjemcovia a slúžia k poskytnutiu informácií online alebo sú obchodným zdeléním ako aj služby platforiem umožňujúce vyhľadávanie prístup a získavanie dát;
- c) služby poskytovania informácií prostredníctvom komunikačnej siete, poskytovanie prístupu k tejto sieti alebo zhromažďovanie informácií poskytovaných príjemcom služby.

Naproti tomu recitál 18 negatívne z výpočtu vymedzuje samotné dodanie tovaru a poskytovanie služieb offline, ako aj televízne a rozhlasové vysielanie. Interpretačnou pomôckou je aj Príloha 5 Smernice č. 98/34/ES osvetľuje ďalšie definičné znaky služby informačnej spoločnosti – *poskytnutie na diaľku*. To nemôže byť za súčasnej prítomnosti jej adresáta, ako napríklad v prípade prehľadávania elektronického katalógu tovaru záujemcom na predajni alebo *poskytnutie elektronicky* nenastáva v prípade vydania požadovanej sumy strojovým bankomatom.

Tieto smernice boli novelizované smernicou Európskeho Parlamentu a Rady (EÚ) 2015/1535 z 9. septembra 2015, ktorou sa stanovuje postup pri poskytovaní informácií v oblasti technických predpisov a pravidiel vzťahujúcich sa na služby informačnej spoločnosti (kodifikované znenie), ktorá v čl. 1 odst. 1 písm. b) definuje službu ako akúkoľvek službu informačnej spoločnosti, tj. každú službu, ktorá sa bežne poskytuje za odmenu, na diaľku, elektronickým spôsobom a na základe individuálnej žiadosti príjemcu služieb. V súhrne si dovoľíme naďalej pracovať práve s touto verziou definičných znakov, ktoré by mali byť *de lege ferenda* na základe európskej úpravy do znenia definície *služieb informačnej spoločnosti* § 2 písm. a) ZoNSIS podľa môjho názoru novelizované.

3.2.2.1 Poskytovanie služieb elektronickými prostriedkami (elektronickým spôsobom)

Znamená, že: „*služba sa z miesta pôvodu odošle a na mieste určenia prijíma prostredníctvom elektronického zariadenia, určeného na spracovávanie (vrátane digitálneho komprimovania) a uskladňovanie údajov a je úplne vysielaná, prenášaná a prijímaná po drôte, prostredníctvom rádiových vĺn, optickým spôsobom, alebo inými elektromagnetickými prostriedkami*“¹⁵⁵. Z povahy tejto definície hovoríme o negatívnom vymedzení podmienky, v ktorej nejde o službu informačnej spoločnosti ak nie je poskytovaná elektronickými prostriedkami v zmysle §2 písm. c) ZoNSIS, ako uvádza dôvodová správa k zákonu. Ide o demonštratívny výpočet software a hardware¹⁵⁶, pre naše potreby, teda hlavne sieť elektronických komunikácií, koncové zariadenie alebo elektronická pošta, ale i *messenger* typu WhatsApp, ICQ a iné prostriedky umožňujúce komunikáciu za súčasnej neprítomnosti strán.

3.2.2.2 Poskytovanie služieb na individuálnu žiadosť užívateľa podanú elektronickými prostriedkami

Definičným kritériom elektronickej žiadosti, ako uvádza Polčák¹⁵⁷ je treba vykladať extenzívne, kedy za takú žiadosť môžeme považovať akúkoľvek aktivitu užívateľa, na ktorého základe je služba poskytovaná. Túto individuálnu žiadosť môžeme chápať aj ako jednotlivú akciu užívateľa smerujúcu k začatiu poskytovania služby¹⁵⁸, ako napríklad prihlásenie do siete alebo do webového rozhrania vpísaním identifikačnej adresy, ale

¹⁵⁵ Čl. 1 písm. b) ii) Smernice Európskeho parlamentu a Rady (EÚ) 2015/1535

¹⁵⁶ Dôvodová správa k zákonu č. 480/2004 Sb., o niektorých službách informačnej spoločnosti a o zmene niektorých zákonů (480/2004 DZ) Sněmovní tisk č. 579/0, Poslanecká sněmovna, 4. volební období. Dostupné z: <http://www.psp.cz/sqw/text/orig2.sqw?idd=12508&pdf=1>. s.14 (ďalej aj ako „*dôvodová správa k ZoNSIS*“)

¹⁵⁷ POLČÁK, Radim. *Právo na internetu: spam a odpovědnost ISP*. Brno: Computer Press, 2007, 160 s. Právo a IT. ISBN 9788025117774, s.49

¹⁵⁸ MAISNER, Martin. *Zákon o některých službách informační společnosti: Komentář*. V Praze: C.H. Beck, 2016. Beckovy komentáře, 223s. ISBN 9788074004490. s.10 marginália č.10 a k elektronickým prostriedkom s.11 marginália č.29

i odoslanie instantnej správy v messengeri. Merítkom je individualita poskytnutej služby, preto teda nepôjde o prípady televízneho vysielania.

3.2.2.3 Poskytovanie služieb spravidla za úplatu

Túto podmienku si nemôžeme vykladať reštriktívne. Je potrebné si uvedomiť, že v mnohých prípadoch nejde o dvojstranný právny vzťah medzi poskytovateľom a užívateľom, v ktorom užívateľ vykonáva transakciu ako v prípade uzavretia zmluvy. Do tohto vzťahu vstupuje potenciál monetizácie individuálnych užívateľských aktivít poskytovateľom. Poskytovateľ môže ťažiť z úhrady a umiestnenie bannerových reklám tovaru na svojich stránkach, ktoré užívateľ frekventovane navštevuje¹⁵⁹. Takýto výklad podporil v rozsudku o štvrtej predbežnej otázke Súdny dvor Európskej Únie z 11. septembra 2014 vo veci C-291/13 Papasavvas: „*pojem „služby informačnej spoločnosti... zahŕňa služby poskytujúce on-line informácie, za ktoré nie je poskytovateľ odmenený príjmom služieb, ale príjmami plynúcimi z reklamy, ktorá sa objavuje na internetovej stránke*“¹⁶⁰.

Ondřej Elterein vo svojej práci¹⁶¹ rozdeľuje služby informačnej spoločnosti ponúkané ich poskytovateľmi do dvoch základných rovín z hľadiska vzťahu k ich príjmom:

- a) Služby, v ktorých príjemcovia vystupujú ako pasívny recipienti poskytovaného obsahu. V takom prípade nie je nutné aplikovať úpravu o zodpovednosti poskytovateľov týchto služieb podľa ZoNSIS, ale naopak, v prípade porušenia povinností nastúpi úprava podľa príslušných právnych predpisov.
- b) Služby a aplikácie, kedy ich príjemcovia vystupujú v dvojakej úlohe - príjemcovia služieb informačnej spoločnosti a zároveň ako aktívni poskytovatelia obsahu týchto služieb (*user generated content*, pozn.). Poskytnutím technických prostriedkov

¹⁵⁹ MAISNER, 2016, op.cit., s.8 marginália č.12

¹⁶⁰ Rozsudok z dňa 11. septembra 2014, Papasavvas, C-291/13, ECLI:EU:C:2014:2209, bod 30

¹⁶¹ ELTEREIN, Ondřej. *Služba informační společnosti v prostředí sítě Internet a autorské právo* [online]. Rigorózní práce. Univerzita Karlova v Praze, Právnická fakulta. Vedúci práce Irena Holcová. 2012, s.63 [cit. 24.3.2018]. Dostupné z: <https://dspace.cuni.cz/handle/20.500.11956/60406>

prostredníctvom, ktorých môže dochádzať k protiprávnemu jednaniu je potrebné skúmať zodpovednosť poskytovateľov služieb informačnej spoločnosti podľa kľúčových ustanovení ZoNSIS.

3.2.3 Poskytovateľ služieb informačnej spoločnosti

Transpozíciou smernice o e-obchode sa do českého právneho poriadku § 2 písm. d) ZoNSIS plne prebrala právna definícia poskytovateľa služby informačnej spoločnosti ako: „každá fyzická alebo právnická osoba, ktorá poskytuje niektorou ze služieb informační společnosti“. V zásade je teda poskytovateľ definovaný pojmovými prvkami služby, ktorú poskytuje, pričom to bude každý subjekt, ktorý zaobstaráva možnosť komunikácie v rámci informačnej siete, alebo sám takúto službu vytvára a spracováva alebo šíri informácie v elektronickej forme¹⁶².

Tieto subjekty v prostredí internetu technicky filtrujú a spracovávajú nielen požiadavky koncových užívateľov, ale taktiež obsah, ktorý im je zobrazovaný, čím sa stavajú do role autority vďaka ktorej jednotliví užívatelia do informačnej siete nielen vstupujú, ale prostredníctvom ktorých prebieha tvorba, spracovanie alebo výmena či šírenie informácií. Pri poukázaní na našu definičnú vertikálnu štruktúru regulácie internetu budú v pozícii tvorcov určitých pravidiel, ktorými zaväzujú stupeň koncového užívateľa. Ide o poskytovateľov prístupu ku komunikačnej sieti, ktorí nastavujú parametre služby alebo poskytovateľov participačných platforiem ako sú sociálne siete, v ktorých užívateľ súhlasí so stanovenými podmienkami ich užívania. V tomto ohľade sa nemôže jednať len o poskytovateľov, ako sú definovaní ďalej §§ 3-5 ZoNSIS, ale aj o všetkých ostatných poskytovateľov, ktorí poskytujú také služby, ktoré spĺňajú kritéria prvkov poskytovanej služby.

V informačnej spoločnosti v spojení s rýchlym progresom vývoja nových aplikácií či internetových platforiem sebarealizácie, nemôže byť akýkoľvek zoznam ISP nerozširujúcim sa definitívom. Krátku predstavu o typoch ISP nám podáva dnes mierne archaický dokument

¹⁶² POLČÁK, *Internet a proměny práva*, 2012, op. cit., s.142

OECD z apríla 2010¹⁶³, ktorý z ekonomického pohľadu rozumie činnosti ISP (používa pojem internet intermediaries, pozn.) ako „sprostredkovanie alebo uľahčenie transakcií uzatvorených tretími stranami na internete. Taktiež umožňujú prístup k, uloženie, prenášanie a indexáciu obsahu, produktom a službám, ktoré na internete vyrobili tretie strany alebo poskytujú internetové služby tretím stranám.“ ISP dokument demonštratívne kategorizuje troma úrovňami s príkladmi, ktoré si dovoľíme aktualizovať viac k európskym pomerom:

Poskytovatelia prístupu k internetu a služieb internetu; drátový i bezdrátový ako i mobilný operátori poskytujúci prístup k internetu (ISP a LAP, viz. nižšie) napr. Verizon, Comcast, Telefónica O2, Orange, T-mobile, BT			
Web Hosting, spracovanie dát a doručovanie obsahu (Web Hostin, Data Processing and Content Delivery) napr. Go Daddy, Bluehost, Wedos, Akamai, Easyspace, Dropbox, blogger			
Internetové vyhľadávače a portály (Search Engines and Portals) napr. Google, Seznam, Yahoo, Bing, MSN	Sprostredkovatelia elektronického obchodovania (E-commerce Intermediaries) napr. Amazon, Alibaba, eBay, Aukro, Mall	Platobné systémy (Payment Systems) napr. Visa, Paypal, PaySec	Participačné sieťové platformy, platformy digitálnej sebarealizácie (Participative Networked Platforms) napr. Facebook, Twitter, Reddit, Instagram, LinkedIn, lide.cz

Dokument OECD podporuje tézu Ondřeja Eltreina o pasívnych a aktívnych príjemcoch služieb informačnej spoločnosti. Na jednej strane využívajú tieto platformy užívatelia – tretie strany taktiež aktívne k tvorbe obsahu, ponúkaniu tovaru a obchodných služieb a na strane druhej sa tvorí kategória čisto pasívnych príjemcov takto poskytnutého obsahu.

3.2.4 Užívateľ služby informačnej spoločnosti

Európska úprava smernice o e-obchode používa distančný pojem príjemca služby informačnej spoločnosti, ktorý sa jasne odlišuje od pojmu spotrebiteľ, okrem zakotvenia

¹⁶³ OECD. *The Economic and Social Role of Internet Intermediaries* [online]. Publikované 4/2017 [cit. 24.3.2018]. Dostupné z: www.oecd.org/internet/ieconomy/44949023.pdf. s.9

definičných znakov v čl. 2 rozširuje prvok pojmu recitálom č. 20 *lato sensu* taktiež na: „osoby, ktoré poskytujú informácie na otvorených sieťach, ako je napríklad internet, alebo osobami, ktoré hľadajú informácie na internete zo súkromných alebo pracovných dôvodov“. V českom právnom prostredí budeme pracovať s pojmom užívateľ ako je definovaný v § 2 písm. d) ZoNSIS ako: „každá fyzická alebo právnická osoba, ktorá využíva službu informační společnosti, zejména za účelem vyhledávání či zpřístupňování informací“.

3.3 Právny koncept zodpovednosti v prostredí internetu podľa Zákona č. 480/2004 Sb.

V komentári k zákonu o informačnej spoločnosti Maisner¹⁶⁴ pojednáva o dvoch základných konceptoch zodpovednosti za obsah sprístupnený prostredníctvom internetu – primárna povinnosť zodpovednosti za vlastný obsah a zodpovednosť za cudzí obsah.

Koncept priamej zodpovednosti za vlastný obsah je základným prípadom jednania poskytovateľa obsahu (nemusí byť len ISP, pozn.), ktorým vytvára a inak nakladá s obsahom, a to na vlastné náklady a z vlastnej pohnútky. Príkladom je publikácia názorového príspevku pôvodného obsahu prostredníctvom svojich vlastných služieb. Za túto činnosť poskytovateľ zodpovedá ako za svoje vlastné jednanie¹⁶⁵.

O obdobný prípad by sa jednalo v prípadoch, kedy by síce poskytovateľ nevytvoril obsah sám, avšak by cudzí obsah prebral alebo prijal takým spôsobom, že je považovaný za pôvodcu obsahu. K tomu najčastejšie dôjde pri preberaní autorských diel, napríklad preložením zahraničného článku do spravodajského denníka, tak že za prebratý obsah odpovedá ako by článok poskytovateľ vytvoril sám, a to i s prípadnou zodpovednosťou porušenia práv tretích osôb¹⁶⁶. Zodpovednosť sa nezaloží poskytovaním vložených odkazov na cudzí obsah. Do úvahy o primárnej zodpovednosti poskytovateľa prichádza úmyselne alebo hrubo nedbalé zabezpečenie prístupu do administrátorského účtu správy webového rozhrania pre publikovanie obsahu do spravodajského denníka, na základe ktorého do účtu niekto vnikne a publikuje protiprávny obsah. Z rozhodnutia Najvyššieho súdu vo veci Prolux

¹⁶⁴ MAISNER, 2016, op.cit., s.33-34 a násl.

¹⁶⁵ JANSÁ, OTEVŘEL, ČERMÁK, MALIŠ, HOSTAŠ, MATĚJKA a Ján MATEJKA, 2016, op.cit., s.141

¹⁶⁶ *ibid*, s.143

Consulting Int, s.r.o. proti Internet Info s.r.o.¹⁶⁷ naopak ISP poskytujúci možnosť pridania diskusných príspevkov užívateľom k publikovanému obsahu nebude za posúdenie obsahu komentára, ktorý potenciálne zasahuje do osobnostných práv človeka zodpovedný.

O koncepte nepriamej zodpovednosti hovoríme v prípadoch zodpovednosti poskytovateľa za cudzí obsah, ktorý je uverejnený v službe ISP jej jednotlivými užívateľmi, ktorí prenosom alebo spracovaním informácie samotný obsah vytvorili a tým sa dopustili porušenia právnych predpisov. Zodpovednosť u ISP prichádza do pozornosti v prípade, kedy s cudzím obsahom z povahy ich podnikania pomáhajú nakladať, napríklad jeho sprístupnením alebo poskytnutím prostriedkov k umožneniu jeho šírenia. V trestnoprávnej teórii môžeme hovoriť o rôznej forme účasti poskytovateľa na jednaní inej osoby¹⁶⁸ vo forme návodu alebo pomoci., kedy príkladne prevádzkovateľ diskusného fóra na internete priamo vyzýval k uverejneniu protiprávneho obsahu ako napríklad výzva k „*hate speech*“, čo môže viesť k trestne právnej zodpovednosti poskytovateľa ako aj užívateľa.

Kvalifikovaným poskytovateľom, ktorí priamo nenakladajú, nerozhodujú o spôsobe využitia obsahu a ich faktická možnosť efektívnej kontroly je obmedzená alebo nonexistentná¹⁶⁹ je potrebné poskytnúť určitý stupeň ochrany obmedzením či vylúčením zodpovednosti za cudzí obsah, a to ako vylúčením trestnej a správnej zodpovednosti tak i súkromnoprávnej povinnosti nahradiť škodu. Tým sa ale nevylučuje možnosť prijatia opatrenia k náprave protiprávneho stavu, o ktorom sa ISP dozvie, napríklad na podnet poškodeného alebo súdneho či správneho orgánu. Protiprávny následok súvisí vo väčšine situácií s porušením autorského práva, avšak vylúčené nie sú oblasti trestného alebo súťažného práva.

¹⁶⁷ Rozhodnutí Nejvyššího soudu České republiky pod sp.zn. 23 Cdo 2623/2011 z dňa 31.7.2013. [cit. 25.3.2018]. Dostupné i online napr. z: <http://kraken.slv.cz/23Cdo2623/2011>

¹⁶⁸ JANSÁ, OTEVŘEL, ČERMÁK, MALÍŠ, HOSTAŠ, MATĚJKA a Ján MATEJKA, 2016, op.cit., s.154

¹⁶⁹ *ibid.* s.157 a násl.

Úpravu zodpovednosti kvalifikovaných typov ISP preberá zo smernice o e-obchode štyrmi kľúčovými ustanoveniami §§ 3 až 6 ZoNSIS, úprava, ktorú je nutné v individuálnych prípadoch aplikovať prednostne pred ostatnými obecnými predpismi, a to vrátane špeciálnych nárokov nahradzujúcich ostatné právne nároky uplatniteľné obecné¹⁷⁰. Dôvodom je dostatočná ochrana podnikania spojeného s poskytovaním služieb informačnej spoločnosti, ako aj ochrana tretích osôb, ktorých práva nemôžu byť týmto spôsobom dotknuté.

Doktrinálnym východiskom úpravy zodpovednosti ISP je teda horizontálny právny prístup vzťahujúci sa na všetok cudzí obsah s výnimkou hazardných hier a ochrany osobnosti a súkromia, nielen na autorskoprávne chránený obsah¹⁷¹, a to vylúčením kvalifikovaných ISP z režimu bežnej zodpovednosti za cudzí obsah pri splnení zákonných predpokladov.

Bežný režim zodpovednosti, by takto predstavoval neúnosnú mieru rizika, ktoré by ISP preberalo v spojení s poskytovaním služieb informačnej spoločnosti. Pri prevádzkovaní služieb do ktorých vstupuje veľký počet jednotlivých užívateľov by sa tak vystavili takmer istej realizácii vzniku zodpovednosti za obsah, ktorý do svojej služby neumiestnili z vlastnej pohnútky. Pričom ich zisk by z jednotlivých interakcií bol zanedbateľný oproti administratívnym nákladom, ktoré by boli spojené so stálym dohľadom obsahu a v prevažnej miere anonymných užívateľov.

Alternatívne by sa ISP stávala za účelom ochrany vlastných záujmov do úlohy autoritatívneho cenzora *ex ante* zablokováním prístupu k obsahu zverejňovaného užívateľmi prostredníctvom platformy na základe vlastného uváženia, čo by evokovalo proverbskú cenzúru slobodného prejavu. Poznamenávame, že určitý stupeň ochrany prevádzkovateľa rôznych diskusných fór alebo sociálnych sietí implementujú tzv. podmienkami používania a pravidiel diskusie, tie sú ale skôr nasmerovaním a nie sú plne vymáhané. Jedno z rizík vyplývajúcim pre ISP pri uvedenom postupe by nastalo v kolízii s verejnoprávnou ochranou

¹⁷⁰ *ibid*, s.34

¹⁷¹ ANDRUŠKO, 2016, op.cit., s.108 a násl.

osobnosti, súkromia a osobných údajov¹⁷². Predstavme si prípad poskytovateľa VoIP ako napr. Skype, kde bežný režim zodpovednosti by v súhrne znamenal zhromažďovanie osobných údajov o všetkých účastníkoch telefonátov, ako i obsahu rozhovorov či poslaných instantných správ. Naproti tomu režim absolútnej nezodpovednosti ISP by vyvolal stav právneho vákua prostriedkov postihnuteľnosti osôb porušujúcich práva tretích osôb, ktorým by bol takto efektívne odmietnutý prístup k ochrane subjektívnych práv.

3.4 Vylúčenie z režimu všeobecnej zodpovednosti

Regulácia výnimiek z režimu bežnej zodpovednosti sa podľa transponovanej smernice a ZoNSIS týka troch kogentne kvalifikovaných poskytovateľov služieb informačnej spoločnosti, na ktorých sa špeciálny ochranný režim nezodpovednosti za vzťahuje za zákonom uvedených podmienok. Tento režim odborne označujeme ako bezpečný prístav (*safe harbour*, pozn.) podľa amerického vzoru¹⁷³. Kľúčové ustanovenia o zodpovednosti nie sú koncipované spôsobom, ktorý by predstavoval nepriamu novelu platných právnych predpisov¹⁷⁴. Ide o blanketné ustanovenie, ktoré všeobecne odkazuje na iné relevantné zákony upravujúce zodpovednosť. Zodpovedajúce normy môžu byť aplikované na zodpovednostné vzťahy verejnoprávne vyplývajúce napríklad zo zákona č. 101/2000 Sb. o ochrane osobných údajov, trestného zákoníka alebo priestupkového zákona ako aj súkromnoprávne (inštitút náhrady škody v občianskom zákoníku). V súvislosti so ZoNSIS nepojednávame o komplexnej úprave zodpovednosti, teda v kontexte

¹⁷² POLČÁK, Radim. Odpovědnost poskytovatelů služeb informační společnosti (ISP). *Právní rozhledy*, Praha: C.H.Beck. 2009, roč. 2009, č. 23, s. 837-841. ISSN 1210-6410

¹⁷³ Pojem *safe harbour* sa vžil z Digital Millennium Copyright Act (DMCA), americkej reformy autorských práv v digitálnom svete. "Bezpečný prístav" je námorná metafora označujúca miesto kde proverbská loď - ISP bezpečne zakotví pred búrlivým počasím – možným porušovaním najmä autorských práv. Ale ako v prípade lode režim mimo bezpečného prístavu neznamená, že je v nebezpečenstve. Znamená to, že bezpečnosť lode nie je právom zaručená. Prevzaté a doplnené. srov. napr. HOLLAAR Lee A., *Legal Protection of digital information* [online]. Publikované 2002 [cit. 25.3.2018]. Dostupné z: digital-law-online.info/lpdi1.0/treatise33.html

¹⁷⁴ Srov. k ust. § 5 a § 6 Důvodová zpráva k zákonu č. 480/2004 Sb., op.cit., s.15

zodpovednostný vzťah pri nesplnení podmienok *safe harbour* vznikne bez ohľadu na druh zverejňovaného obsahu.

Táto úprava sa v prípade vzniku zodpovednostného vzťahu uplatní individuálne pre všetky právne odvetvia a medzi-odvetvia. Inštitút vylúčenia zodpovednosti, ako uvádza Husovec¹⁷⁵, ale nemá zakladať zodpovednosť k cudziemu obsahu v prípade straty režimu bezpečného prístavu. Cieľom tejto úpravy je určiť moment, dokiaľ zodpovednosť za konanie užívateľa nemožno uplatniť a ak sa ustanovenia §§ 3-5 Zákona o SIS neaplikujú, dôvod uplatnenia zodpovednosti poskytovateľa bude súdny alebo správny orgán aplikovať podľa vnútroštátnych noriem. Mätúcim je použitie formulácie „*poskytovateľ zodpovedá ak*“¹⁷⁶ českým zákonodarcom, čím vzbudzuje dojem, že strata bezpečného prístavu znamená automaticky aj vznik zodpovednosti¹⁷⁷.

Ako sme uviedli, vylúčenie zodpovednosti podľa článkov § 3 až 5 ZSIS sa dotýka všetkých typov zodpovednosti, t.j. občianskoprávnej, správnoprávnej ako aj trestnoprávnej. Pri niektorých podmienkach bezpečného prístavu však môže existovať diferencovaný prístup pokiaľ ide o civilnú zodpovednosť na jednej strane a zodpovednosť správnoprávnú a trestnoprávnú na strane druhej. Bezpečné prístavy, podľa vyššie uvedených ustanovení, navyše v oblasti občianskej, administratívnej, ale aj trestnej nebránia verejným mocenským orgánom v tom, aby mohli prikázať poskytovateľovi služieb ukončenie alebo predchádzanie porušovania predpisov v poskytovanej službe. Na takýto príkaz musí mať súd alebo správny orgán prirodzene najprv právomoc vo vnútroštátnom práve. K tomu sa vzťahuje určitá podmienka nevedomosti o protiprávnosti, podobne ako v prípade Prolux v. Internet Info, po strate nevedomosti o protiprávnosti obsahu alebo jednania môže, avšak nie nutne musí vykonať kroky smerujúce k odstráneniu alebo znepriístupneniu obsahu.

V oblasti občianskej zodpovednosti to znamená, že súd môže poskytovateľovi služby prikázať určité konanie aj vtedy, ak je chránený bezpečným prístavom voči inej

¹⁷⁵ HUSOVEC, Martin. *Zodpovednosť na internete: podľa českého a slovenského práva*. Praha: CZ.NIC, 2014, 234 s. ISBN 9788090424883. s.95

¹⁷⁶ Nepreložene zo ZoNSIS „*jen pokud*“

¹⁷⁷ *ibid*, s. 94

zodpovednosti. Súd tak môže v prípade, ak na strane žalobcu existuje hmotnoprávny nárok alebo procesnoprávne oprávnenie, prikázať poskytovateľovi poskytnúť určité informácie o svojich užívateľoch alebo dokonca implementovať určité technické riešenie.

Režim bezpečného prístavu je funkčne zákonom limitovaný na ISP uvedených v §§ 3 až 5 ZoNSIS, teda nasledujúce poskytované služby, z ktorých bližšiemu rozboru podrobíme poskytovateľa v § 3:

- (i) Jednoduchý prenos (*mere conduit*), teda službu, ktorá spočíva v prenose informácií poskytnutých užívateľom prostredníctvom komunikačnej siete, alebo sprostredkováva prístup k sieti za týmto účelom (srov. §3 ZoNSIS a čl. 12 smernice o e-obchode),
- (ii) Ukladanie do vyrovnávacej pamäte (*caching*), teda službu, ktorá spočíva v prenose obsahu informácií, ktoré slúžia výhradne pre čo možno najúčinnější následný prenos týchto informácií na žiadosť iných užívateľov (srov. §2 písm. h) v spojení s §4 ZoNSIS, čl. 13 smernice o e-obchode), a
- (iii) Zhromažďovanie informácií (*hosting*), teda službu, ktorá spočíva v ukladaní informácií poskytnutých užívateľom (srov. §5 ZoNSIS, čl. 14 smernice o e-obchode).

3.4.1.1 Výlučenie povinnosti dohľadu

Ako uvádza dôvodová správa k ZoNSIS¹⁷⁸, nie je rozumné od ISP požadovať posúdenie legálnosti a nelegálnosti celého obsahu uložených informácií, preto im nie je uložená povinnosť aktívne monitorovať materiály uložené na ich serveroch, a to ani *ex post* po zverejnení obsahu. Tým by bolo porušené pravidlo nemonitorovania obsahu užívateľsky prenášaných a ukladaných informácií za účelom odhaľovania protiprávnej činnosti, alebo povinnosti obstarávať dôkazy svedčiace o protiprávnosti podozrivého obsahu informácie *ex post*¹⁷⁹. Táto činnosť je v rámci ekonomickej optimalizácie prenesená na autoregulačné

¹⁷⁸ Srov. Dôvodová správa k zákonu č. 480/2004 Sb., op.cit., s. 15

¹⁷⁹ HUSOVEC, 2014, op.cit., s.35

mechanizmy manuálneho dohľadu vlastníkov práv, ktoré môžu byť užívateľskou činnosťou dotknuté a prípadne do samotnej kompetencie dozorného orgánu. Manuálny dohľad nad obsahom môžu poskytovať i tretie strany prostredníctvom tzv. rodičovským zámkom, a tým z rozhodnutia užívateľa blokovat' určitý obsah¹⁸⁰. Jedná sa o úpravu v ustanovení §6 ZoNSIS:

„§ 6

Poskytovatelé služeb uvedení v § 3 až 5 nejsou povinni

- a) *dohlížet na obsah jimi přenášených nebo ukládaných informací,*
- b) *aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace.“*

Táto doktrína je vo vzťahu k ISP poskytujúcim verejne dostupnú službu elektronických komunikácií (teda službu prenosu obsahu, pozn.) k obsahu prenášaných správ zmienená i v §61 odst. 5) ZoElKom. Z regulatorného hľadiska je to jedným zo základov nediskriminačného prístupu podnikania subjektov v elektronických komunikáciách, kde by opak tejto formulácie predstavoval ekonomickú bariéru prístupu.

Systematický doplnok *safe harbour* zabraňuje vzniku povinnosti kvalifikovaných ISP obecného dohľadu nad obsahom prameniatiemu z rozhodnutia verejného orgánu (súdu a kontrolných orgánov) a obecných právnych predpisov¹⁸¹. Recitál 47 smernice o e-obchode upozorňuje, že vylúčenie dohľadu: „*sa netýka povinností monitorovať v špecifickom prípade, a najmä nemá vplyv na nariadenia vnútroštátnych orgánov v súlade s vnútroštátnymi predpismi*“.

Čo je obecný dohľad približuje napríklad rozsudok Súdneho dvora Európskej únie vo veci Scarlet proti SABAM C-360/10¹⁸². Zvláštny dohľad by svojou špecifickosťou nenaplňal

¹⁸⁰ Bližšie k možnostiam technického a manuálneho blokovania prístupu k obsahu viz. kapitola 4.3

¹⁸¹ Prezaté MAISNER, 2016, op.cit., s.99 a násl.

¹⁸² Z Rozsudku Súdneho dvora EU z dňa 16. februára 2012, SABAM proti Netlog NV, C-360/10, ECLI:EU:C:2012:85, bod 26

„vzhľadom na požiadavky vyplývajúce z ochrany uplatniteľných základných práv sa majú vykladať v tom zmysle, že bránia vydaniu súdneho príkazu vnútroštátnym súdom, ktorý by poskytovateľovi hostingových služieb ukladal povinnosť zaviesť systém filtrovania (i) informácií ukladaných na jeho serveroch používateľmi

znaky uvedené v judikáte, i keď tie nie sú dostatočne reštriktívne uvedené, a bol by uložený vnútroštátnymi orgánmi s prihliadnutím k individuálnym okolnostiam, právnej úpravy proporcionality ochrany ľudských práv a súkromného života¹⁸³. Príkladom by mohlo byť rozhodnutie správneho orgánu priamym uložením povinnosti ISP blokovať prístup k špecifickému nezákonnému obsahu napríklad stránkam poskytujúcim pornografický obsah v rozpore so zákonom v prevádzke komunikačnej siete.

3.4.2 Mere conduit

Ide o podmnožinu poskytovateľov, ktorí poskytujú službu spočívajúcu v prenose dát vykonávaným ako služba pre tretie osoby¹⁸⁴. Takýto prenos musí byť prostý, teda bez akýchkoľvek zásahov alebo vstupu ISP do obsahu prenášanej informácie alebo iniciácie prenosu na vlastný podnet. Praktickým výkladom môžeme túto množinu rozdeliť na ISP, ktorí užívateľom poskytujú:

- a) Služby spočívajúce v sprostredkovaní prístupu k infraštruktúre siete elektronickej komunikácie, čo budú služby poskytovateľov pripojenia k internetu (IAP, pozn.) podľa ZoElKom¹⁸⁵, ale taktiež nelicencovaný poskytovatelia bezdrôtového pripojenia v reštauračných a obdobných zariadeniach.
- b) Služby spočívajúce v pripojení sa do sieťovej infraštruktúry za účelom využitia určitej aplikácie k prenosu informácií, čo budú hlavne služby prenosu hlasu ako Skype, alebo *instant messenger*, ktoré centralizované informácie neukladajú na servery, ktoré sú dnes skôr raritou, alebo emailové systémy využívajúce protokol POP3 automatického zmazania správ po stiahnutí užívateľom napr. Microsoft Outlook.

jeho služieb, (ii) ktorý sa bude uplatňovať bez rozdielu na všetkých jeho používateľov, (iii) preventívne, (iv) výlučne na jeho náklady, (v) bez časového obmedzenia spôsobilý identifikovať elektronické súbory ... s cieľom blokovať sprístupnenie uvedených súborov, ktorých výmena porušuje autorské právo, verejnosti“

¹⁸³ MAISNER, 2016, op.cit., s.119, marginália č.77

¹⁸⁴ JANSÁ, OTEVŘEL, ČERMÁK, MALIŠ, HOSTAŠ, MATĚJKA a Ján MATEJKA, 2016, op.cit., s.175

¹⁸⁵ Poskytovatelia káblového pripojenia ako UPC al. O2, mobilní operátori ako Vodafone, pozn.

Poskytovateľ vstupuje do prenosu vždy pasívne, sprostredkovaním pripojenia do siete elektronickej komunikácie¹⁸⁶, alebo prenosom informácie po tejto sieti na individuálnu žiadosť príjemcu – vytočením kontaktu v adresári programu určeného k internetovému volaniu Skype. Ako uvádza dôvodová správa k ZoNSIS, po tomto type kvalifikovaného poskytovateľa nie je možné technicky požadovať, aby sledoval protiprávne kroky jednotlivých užívateľov, ako napríklad prenos detskej pornografie alebo šírenie nacistických myšlienok.

Poskytovateľ jednoduchého prenosu stratí privilégium režimu bezpečného prístavu pri nesplnení podmienok §3 ZoNSIS a zodpovednosť za obsah prenášanej informácie bude predmetom ďalšieho posúdenia súdneho alebo správneho orgánu¹⁸⁷. Z povahy tejto služby je zrejmé, že ISP tohto typu má limitované možnosti kontroly prenášaného obsahu a základom je teda zákaz akéhokoľvek zásahu do prenášaného obsahu. Transpozícia smernice o e-obchode znie:

„§ 3

(1) *Poskytovatel služby, jež spočívá v přenosu informací poskytnutých uživatelem prostřednictvím sítí elektronických komunikací nebo ve zprostředkování přístupu k sítím elektronických komunikací za účelem přenosu informací, odpovídá za obsah přenášených informací, jen pokud*

- a) *přenos sám iniciuje,*
- b) *zvolí uživatele přenášené informace, nebo*

¹⁸⁶ Český zákonodárca neprebral názvoslovie používané Smernicou o e-obchode – komunikačná sieť, pozn.

¹⁸⁷ Ako bolo spomenuté v kapitole 3.4 strata režimu bezpečného prístavu nezakladá automaticky verjenoprávnu ani súkromnoprávnu zodpovednosť ISP. Ide o zcela odlišné inštitúty práva. Ako uvádza Maisner v komentári k Zákonu o SIS vylúčenie zodpovednosti bolo do českého právneho poriadku ako bolo spomenuté vyššie transponované na základe smernice 2000/31 transponované chybné. Z gramatického výkladu aktuálneho znenia príslušných odstavcov nám plyní založenie zodpovednosti v uvedených prípadoch, nie jej vylúčenie. Táto nepresnosť bola odbornou verejnosťou niekoľkokrát kritizovaná, na nápravu legislatívnej chyby však neprišlo (srov. napr. HARAŠTA, Jakub. Obecná prevenční povinnost poskytovatele služeb informační společnosti ve vztahu k informacím ukládaným uživatelem. *Právní rozhledy*, Nakladatelství C.H. Beck. 2014, roč. 2014, č. 17, s. 590-593. ISSN 1210-6410; POLČÁK, *Internet a proměny práva*, 2012, op. cit., s.144–151). I pri požiadavku eurokonformnému výkladu budem v tejto práci pracovať primárne so znením ako ho transponoval český zákonodárca zákonom č.480/2004 Sb., vzhľadom k tomu že prípadné významové odchýlky samotný význam vylúčenia zodpovednosti zásadne nemodifikujú.

c) zvolí nebo změni obsah přenášené informace.

(2) Přenos informací a zprostředkování přístupu podle odstavce 1 zahrnuje také automatické krátkodobě dočasné ukládání přenášených informací.

Zákon doplňa, že taktiež automatické, dočasné medzi-uloženie informácií počas prenosu v časovej dĺžke technologicky obvyklej neznamená, že sa už o prostý prenos informácií nejedná, čo by zodpovedalo práve službám *instant messenger* alebo emailových klientov POP3.

V prípade splnenia týchto podmienok teda poskytovateľ *mere conduit* nezodpovedá za obsah prenášaných informácií. Toto vylúčenie zodpovednosti však pôsobí najmä vo vzťahu k monetárnym nárokom. Pokiaľ ide o odstránenie, zdržovací či informačný nárok, znenie transponovanej smernice o e-obchode v čl. 12 odst. 3 zdôrazňuje, že toto ustanovenie nemá vplyv na „*možnosť, aby súd alebo správny orgán požiadal poskytovateľa služieb, v súlade s právnymi systémami členských štátov, aby ukončil alebo predchádzal porušovaniu predpisov*“. To sa odráža napríklad v ust. § 10 písm. g) ZoElKom a je základom akéhokoľvek blokovania prístupu k obsahu požadovanému po tomto type ISP.

Ako uvádza Husovec vo svojom komplexnom pojednaní o zodpovednosti¹⁸⁸ pre prípad, v ktorom súd môže uložiť povinnosť ukončiť alebo predchádzať porušovaniu predpisov, musí na strane žalobcu existovať hmotneprávny nárok, z ktorého je poskytovateľ pasívne legitimovaný alebo aspoň procesneprávne oprávnenie súdu v konaní, ktoré môže zahájiť. V zásade platí, že pasívne legitimovaná z nároku je len osoba, ktorá cudzie práva porušila. To sa však snaží úijné právo prekonať tým, že týmto poskytovateľom ukladá povinnosť na základe uvádzaných nárokov, bez ohľadu na ich vlastnú zodpovednosť. Takto uložená povinnosť má teda „mimo-zodpovednostný“ charakter, keďže poskytovateľ služby *mere conduit* má povinnosť napr. blokovať nejakú stránku, a to na základe zdržovacieho nároku poškodeného, s ktorým poskytovateľ nie je v deliktuálnom vzťahu.

Zaujímavým je Rozhodnutie Súdneho dvoru EU o blokovaní celých stránok vo veci C314/12 kolokviálne nazývaného UPC Telekabel Wien¹⁸⁹. Súdny dvor Európskej Únie riešil

¹⁸⁸ HUSOVEC, 2014, op.cit., s.127 a násl.

¹⁸⁹ Rozsudok Súdneho dvoru EU z dňa 27. marca 2014, UPC Teleabel Wien GmbH proti Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbh, C-314/12, ECLI:EU:C:2014:192

či je poskytovateľ internetového pripojenia ISP sprostredkovateľom¹⁹⁰, ktorému môže byť na základe súdneho príkazu uložená povinnosť zamedziť prístup svojim zákazníkom k určitým stránkam, ktoré porušujú predmety ochrany autorského práva. Pre túto prácu dôležitá časť SDEU v rozsudku uviedol, že blokovanie stránok s nelegálnym obsahom vytvára kolíziu chránených základných práv, a teda je nutné ich vykladať takým spôsobom, ktorý zaistí spravodlivú rovnováhu medzi rôznymi základnými právami chránenými unijným právnym poriadkom. Konkrétne dovodil kolíziu medzi autorskými právami a právami s nimi súvisiacimi, ktoré sú súčasťou práv duševného vlastníctva v čl. 17 odst. 2 a slobody podnikania poskytovateľa na základe čl. 16, oba články v Charte základných práv Európskej únie. SDEU dovodil pri posúdení vplyvu súdneho príkazu na podnikanie, že taký postup je možný, nakoľko významne neobmedzuje slobodu podnikania, avšak tento príkaz musí ponechať možnosť voľby technických prostriedkov na subjekte ISP. Takéto opatrenie musí byť striktne namierené proti stránkam, ktoré autorské práva porušujú, bez toho aby boli obmedzení ostatní užívatelia ISP v oprávnenom prístupe k informáciám. Overenie zamedzenia adresátom príkazu prístupu je potom na vnútroštátnych orgánoch a prípadne súdoch.

¹⁹⁰ Podľa čl. 8 odst. 3 Smernice Evropského parlamentu a Rady 2001/29/ES z 22. mája 2001 o zosúladení niektorých aspektov autorských práv a s nimi súvisiacich práv v informačnej spoločnosti, : „Členské štáty zabezpečia, aby nositelia práv mali možnosť žiadať o súdny zákaz proti sprostredkovateľom, ktorých služby využívajú tretie strany na porušovanie autorského práva alebo s ním súvisiaceho práva“.

4 Prístup k otvorenému internetu a blokovanie prístupu k obsahu

Jednou z ústredných tém v prostredí internetu, ktorou sa stretáva ochrana základných ľudských práv, najmä na slobodu prejavu a štátny záujem regulácie nevhodného alebo až nezákonného obsahu je prístup k otvorenému internetu. Pojem známy hlavne pod anglickým moniker „*Net Neutrality*“¹⁹¹. Net Neutrality je pojmový prvok koncipovaný v roku 2002, ktorý profesor práva, Tim Wu, zaviedol v diskusii o prekážkach, ktorým čelí každá snaha o reguláciu internetu: *"Akým princípom možno zladit' legítimne záujmy širokopásmových poskytovateľov [pripojenia] pri správe ich siete s nebezpečenstvom poškodenia trhov s novými aplikáciami? A ako sa môže takýto princíp premietnuť do jasných právnych smerníc, ako aj do praxe dizajnu siete?"*¹⁹² Zásady zákazu diskriminácie¹⁹³ a Net Neutrality¹⁹⁴ ako ju definuje Wu inšpirovali FCC¹⁹⁵ k prijatiu novej politiky¹⁹⁶ k adoptácii záväzkov otvoreného a prepojeného internetu v roku 2005. Následne sa v roku 2009 pripojila do diskusie

¹⁹¹ Tiež „siet'ová neutralita“, pozn.

¹⁹² WU Tim. *A proposal for Network Neutrality* [online]. Publikované 6/2002 [cit. 25.3.2018]. Dostupné z: www.timwu.org/OriginalNNProposal.pdf. s.1

¹⁹³ *ibid.* s.2 *"Zásada nediskriminácie funguje tak, že sa rozlišuje medzi obmedzeniami lokálnej siete, všeobecne prípustnými obmedzeniami a obmedzeniami medzi sieťami, ktoré sa považujú za podozrivé. Zásada predstavuje v konečnom dôsledku úsilie vyvinúť zakázané a prípustné dôvody diskriminácie v obmedzeniach používania širokopásmového pripojenia "*

¹⁹⁴ *ibid.* s.2 *"zakázalo by poskytovateľom širokopásmového pripojenia, ak by nepreukázali škodu, od obmedzovania toho, čo používatelia robia s ich internetovým pripojením, a zároveň poskytli poskytovateľovi všeobecnú slobodu riadiť spotrebu šírky pásma a iné záležitosti miestneho záujmu. Princíp [Net Neutrality] dosahuje zákazu vytvorením "zakázaných" a "prípustných" dôvodov na diskrimináciu medzi paketmi v jeho sieti. "*

¹⁹⁵ FCC – Federal Communications Commission. *"Federálna komisia pre komunikáciu reguluje medzištátnu a medzinárodnú komunikáciu prostredníctvom rozhlasu, televízie, drôtov, satelitov a káblov vo všetkých 50 štátoch, v okrese Columbia a amerických územiach." Nezávislá americká vládna agentúra dohliadaná Kongresom je komisia primárna orgán pre komunikačné právo, reguláciu a technologické inovácie "* [cit. 25.3.2018] Prebraté a preložené z: <https://www.fcc.gov/about-fcc/what-we-do>

¹⁹⁶ FCC. *FCC Adopts Policy Statement. New principles preserve and promote the Open and Interconnected Nature of Public Internet* [online]. Publikované 5.8.2005 [cit. 25.3.2018]. Dostupné z: apps.fcc.gov/edocs_public/attachmatch/DOC-260435A1.pdf

o otvorenom internete EÚ pripojením problematiky k Európskej regulačnej agende, s cieľom podporiť niektoré členské štáty, aby ďalej rozpracovali národné prístupy k neutralite siete. V apríli 2014 prijal Európsky parlament v prvom čítaní návrh politiky reformácie telekomunikačného trhu s názvom *Connected Continent*¹⁹⁷, vrátane ustanovení o neutralite siete, ktoré zakazujú zavádzanie diskriminačných opatrení prevádzky vo verejných elektronických sieťach. Diskusia o prísnych predpisoch týkajúcich sa neutrality siete sa stala predmetom prebiehajúcej svetovej diskusie s valným odporom hlavne veľkých IAP, ktorí zvažujú ako odpoveď k týmto pravidlám napríklad spomalenie budovania novej infraštruktúry mobilnej siete 5G¹⁹⁸ a nadnárodný prístup k internetu zaznamenal mnoho rôznych interpretácií pojmu Net Neutrality¹⁹⁹.

Predstavíme viaceré prístupy k tejto téme od európskeho k českému národnému rámcu. O legislatívnu kulmináciu záväzkov jednotného regulačného rámca sa Európska Únia pokúsila až relatívne nedávno. I keď má regulačné úsilie formu nariadenia, a teda je priamo uplatniteľným v členských štátoch, na posúdenie dopadu na budúcnosť je s ohľadom na živú problematiku a rýchle zmeny názorov v americkom legislatívnom prostredí priskoro. Členské štáty aplikujú ustanovenia nariadenia alebo transponujú smernice do národnej legislatívy v praxi len neurčito a pomaly. Problémom môže byť relatívne zložitý výklad problematiky a nedostatok poskytnutých metodických materiálov.

¹⁹⁷ "Tento návrh ukončí diskriminačné zablokovanie a obmedzenie a poskytne účinnú neutralitu siete. Ide o širší spôsob, ako opatrenie v USA (čo nebráni blokovaniu alebo škrteniu služieb, ako napríklad VOIP na mobilných telefónoch). Stanovuje jasné pravidlá pre riadenie prevádzky, ktoré musia byť nediskriminačné, primerané a transparentné". Citácia z DG Connect. *Connected Continent legislative package*. EC.europa.eu, publikované 12.9.2013 [cit. 25.3.2018]. Dostupné z: ec.europa.eu/digital-single-market/en/connected-continent-legislative-package

¹⁹⁸ OPAM Kwame. Major telecoms promise 5G networks if EU cripples net neutrality [online]. *TheVerge*, *ArsTechnica*, publikované 12.7.2016 [cit. 25.3.2018]. Dostupné z: www.theverge.com/2016/7/10/12139700/telecom-companies-5g-service-european-union-net-neutrality

¹⁹⁹ K rôznosti perspektív odborných článkov pre a proti Net Neutrality napr. dostupné online z: journalistsresource.org/studies/society/internet/net-neutrality-debate-underlying-dynamics-research-perspectives

Touto časťou bližšie predstavíme súčasnú reguláciu prístupu k otvorenému internetu a odpovedajúce povinnosti zaväzujúce ISP. Keďže otvorený internet je určitou chimérou, do ktorého tak ľahko vstupujú šíritelia závadného obsahu špecificky sa budeme venovať možnostiam, ktoré sú priznané štátnym orgánom ako aj poskytovateľom nevhodný obsah blokovať, filtrovať alebo odstraňovať. Ďalej predstavíme modely regulačného prístupu s praktickou aplikáciou na prostredie Českej republiky. Opierať sa budeme o porovnávaciu štúdiu týkajúcu sa filtrovania, blokovania a odstraňovania nezákonného obsahu na internete, ktorú na poverenie Rady Európy spracoval Švajčiarsky inštitút komparatívneho práva v jej 47 členských štátoch²⁰⁰.

4.1 Prístup k problematike otvoreného internetu v Európskej únii

Jedným zo základných východísk európskeho chápania otvoreného prístupu k internetu môžeme dohľadať v spomenutej politike EÚ pod názvom *Connected Continent*. I keď je príznačné že všetky sektorové odvetvia sú závislé na kvalitnom pripojení ku sieti elektronickej komunikácie²⁰¹, kulminácia do prijatých legislatívnych záväzkov nebola jednoduchá. Úvodné znenie legislatívne ambiciózneho návrhu sa nestretlo s valnou podporou členských štátov, preto bolo dňa 25. novembra 2015 prijaté s len pomerne okliešteným rozsahom ako Nariadenie Európskeho Parlamentu a Rady (EÚ) 2015/2120²⁰² z pôvodného rozsahu zúžené na témy odstránenia roamingových príplatkov mobilných služieb

²⁰⁰ Swiss Institute of Comparative Law (SICL). *Comparative Study on blocking, filtering and take-down of illegal internet content* [online]. Publikované 20.12.2015, Lausanne [cit. 11.3.2018]. Dostupné z:

<https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content.html>. (Ďalej len ako “Komparatívna štúdia SICL”).

²⁰¹ DLA Piper. *EUROPE: New Telecom Package Promoting Net Neutrality Principle Adopted on October 27th, 2015*. Technology Legal Edge, publikované 2.12.2015 [cit. 11.3.2018]. Dostupné z: www.technologysleage.com/2015/12/europe-new-telecom-package-promoting-net-neutrality-principle-adopted-on-october-27th-2015/

²⁰² Nariadenie Európskeho Parlamentu a Rady (EÚ) 2015/2120 z 25. novembra 2015, ktorým sa ustanovujú opatrenia týkajúce sa prístupu k otvorenému internetu a ktorým sa mení smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb a nariadenie (EÚ) č. 531/2012 o roamingu vo verejných mobilných komunikačných sieťach v rámci Únie.

elektronických komunikácií a pre naratívum tejto kapitoly podstatnú problematiku prístupu k otvorenému internetu v Európskej Únii²⁰³.

V nadväznosti na smernicu o e-obchode pripomeňme, že poskytovatelia prístupu k internetu, sú definovaní práve službou ktorú poskytujú²⁰⁴. Článkom 2 odst. 1 a 2 Nariadenia (EÚ) 2015/2120 zdôvodníme, že službou prístupu k internetu sa mieni poskytovanie verejne dostupnej elektronickej komunikačnej služby. Aplikáciou definícií článku 2 na české právne realie podoprieme výklad primárnou aplikáciou na subjekty, ktoré v zmysle ust. §13 ZoElKom oznámili Českému telekomunikačnému úradu zahájenie činnosti, ktorá je podnikaním v elektronických komunikáciách napr. poskytovaním (verejne dostupnej) služby elektronických komunikácií a túto činnosť reálne vykonávajú.²⁰⁵ Analogicky k výkladu zodpovednosti za obsah informácií môžeme vnímať poskytovateľa pripojenia i ako podmnožinu poskytovateľov služieb informačnej spoločnosti v zmysle ust. § 2 odst. písm. a) a d) zákona o NSIS, hlavne vo vzťahu k poskytovateľom tzv. *mere conduit*.

Ďalším dôležitým pojmom je aj „*služba prístupu k internetu*“, ktorú čl. 2 odst. 2 Nariadenia 2015/2120 vzťahuje na poskytovanie služieb prístupu na internet a špecializovaných služieb. Pokiaľ ide o služby prístupu na internet, ide o verejne dostupné elektronické komunikačné služby, ktoré poskytujú prístup na internet, a tým aj konektivitu prakticky ku všetkým²⁰⁶ koncovým bodom internetu, bez ohľadu na sieťové technológie

²⁰³ Článok Českého telekomunikačného úradu. *Mezinárodní roaming a síťová neutralita v roce 2017* [online]. itPoint, publikované 28.12.2015 [cit. 10.3.2017]. Dostupné z: <http://www.itpoint.cz/ctu/clanky/?i=mezinarodni-roaming-sitova-neutralita-2017-10664>

²⁰⁴ Viz. bod 3.2.2 a násl. tohto dokumentu

²⁰⁵ Srov. ust. § 2 písm. n) a o) ZoElKom. Pre výraz je v angličtine bežne zaužívaný i výraz „*Internet Access Provider*“ známy pod skratkou „*IAP*“, ktorý budeme používať pre naše potreby lepšieho odlíšenia poskytovateľa prístupu k internetu podľa Nariadenia (EÚ) 2015/2120 od poskytovateľa služieb informačnej spoločnosti podľa transponovanej smernice o e-obchode do ZoNSIS, pre ktorý používame skratku „*ISP*“. V zásade sa ale jedná o tie isté subjekty, IAP je prípadne v americkom výklade technickou podmnožinou ISP, kdežto v EÚ sa používa pojem ISP. IAP je teda taktiež ISP.

²⁰⁶ Slovo „prakticky všetkým“ nie je zvolené náhodne. Poskytovateľ prístupu umožňuje prístup k relatívne úzkej časti internetu s predpokladom, že nie všetky časti internetu sa dajú dosiahnuť v akúkoľvek dobu, a to z dôvodov mimo jeho kontroly, napr. v dôsledku cenzúry alebo odlišnej regulácie prístupu v iných krajinách.

(napr. prístup cez fiber, DSL kábel, mobilnú LTE sieť) a bez ohľadu na koncové zariadenie (napr. mobilný telefón, tablet alebo prenosný počítač).

Práva vyplývajúce z nariadenia č. 2015/2120 sa vzťahujú na obidva typy užívateľov²⁰⁷, súhrnným označením koncový užívateľ, a to pre jednotlivých spotrebiteľov, ako aj pre spoločnosti využívajúce služby prístupu na internet. Spoločnosti ako poskytovatelia obsahu a aplikácií (anglická skratka *Content and Application Providers - CAP*, pozn.) požívajú túto ochranu, v prípade používania internetovej služby na poskytovanie obsahu alebo aplikácií iným koncovým užívateľom. CAP je teda typ spoločnosti s obchodnou činnosťou sprístupňovania obsahu na internete (napríklad webové stránky, blogy, video) a / alebo aplikácie (napríklad vyhľadávače, aplikácie VoIP) a / alebo služby²⁰⁸.

Východzia doktrína otvoreného internetu v zmysle recitálov 3, 4 a 6 Nariadenia (EÚ) 2015/2120 je stanoviť spoločný regulačný rámec EÚ pre nediskriminačný prístup užívateľa k informáciám a právo ich šíriť a využívať, napríklad aj poskytovaním aplikácií alebo využívaním iných možností siete internet. Okrem toho je ISP generálne zakázané obmedziť alebo zasahovať do dátovej prevádzky - hlavne blokovaním alebo tzv. „*throttling*“, čiže spomaľovaním rýchlosti prenosu určitých služieb informačnej spoločnosti - alebo s nimi zaobchádzať nerovnomerne a diskriminačne. Táto povinnosť platí bez ohľadu na prvého odosielateľa a koncového príjemcu, použité koncové zariadenie alebo špecifický, samozrejme zákonom povolený obsah, ktorý je v internetovej sieti sprístupnený alebo distribuovaný²⁰⁹. Predpokladom je teda užívateľská možnosť spojenia sa s ostatnými koncovými bodmi či zdrojmi siete internet s ktorými chce komunikovať.

V nadväznosti na výklad o zodpovednosti ISP *mere conduit* by sme mohli hovoriť o princípe rovnakého zaobchádzania s obsahom bez rozlišovania zdroja a cieľa prenosu informácií. Je potrebné upozorniť, že týmto nie je dotknutý režim súkromnoprávnej,

²⁰⁷ Bližšie sme rozobrali aktívnych a pasívnych užívateľov v bode 3.2.2.3a)a)b)

²⁰⁸ Body of European Regulators of Electronic Communications (BEREC, pozn.). *What is covered and protected by the regulation* [online]. [cit. 13.3.2018]. Dostupné z: berec.europa.eu/eng/netneutrality/regulation/

²⁰⁹ GRASSL Gunther. *New EU-Wide Safeguards for Open Internet – EU Regulation 2015/2120* [online]. Schoenherr, publikované 17.1.2017 [cit. 10.3.2018]. Dostupné z: www.lexology.com/library/detail.aspx?g=5e4ee4fc-f15b-4369-865e-5fc35a8e9af2

trestnoprávnej a správnoprávnej zodpovednosti rozvinutý v časti 3, ako priamo uvádza Nariadenie (EÚ) 2015/2120 v článku č. 3 odst. 1: „...nie je dotknuté právo Únie alebo vnútroštátne právo, ktoré je v súlade s právom Únie pokiaľ ide o zákonnosť obsahu, aplikácií alebo služieb“. Recitál 10 sa ďalej stotožňuje z východiskovou zásadou nemonitorovania špecifického obsahu dát poskytovateľmi služieb prístupu k internetu.

4.1.1 Zabezpečenie prístupu k otvorenému internetu

Pre úplnosť považujeme za nutné interpretovať článok 3 Nariadenia (EÚ) 2015/2120, ktorý primárne obsahuje ustanovenia určené na zabezpečenie otvoreného prístupu na internet, ktoré sa vzťahujú jednak k právam koncových užívateľov a v druhom rade upravuje povinnosti a povolené postupy pre poskytovateľov internetových služieb^{210, 211}:

- a) Článok 3 odst. 1 stanovuje práva koncových užívateľov služieb IAP k rovnému prístupu k informáciám a obsahu²¹², právo využívať a poskytovať aplikácie a služby²¹³, a to pomocou koncového zariadenia podľa vlastného výberu;
- b) Článok 3 odst. 2 určuje limity zmluvných podmienok, ktoré sa môžu uplatňovať na poskytované služby a obchodné praktiky IAP. V prvom rade sa ukladá podmienka neobmedzovania celku práv koncového užívateľa stanovených v odst. 1. V súlade s nediskriminačným prístupom k internetu Nariadenie (EÚ) 2015/2120, ale dáva určité práva i samotným IAP, v prvom rade je to možnosť uzatvorenia zmlúv s koncovými užívateľmi o obchodných a technických

²¹⁰ Pre ďalší výklad použijeme skratku „BEREC Guidelines“; BEREC. *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. BoR(16)127*. Publikované August 2016 [cit. 9.3.2018]. Dostupné: berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules;

²¹¹ BEREC Guidelines, 2016, op.cit., Srov. výčet ustanovení článku 3 na s.7 marginália 19 a následný výklad po s. 26 marginália 93.

²¹² Sú tým vymienené teda akékoľvek formy dát, ktoré môžu byť prenášané cez internet; pozn.

²¹³ Sú tým vymienené teda všetky formy klientského a serverového software ako aj služby napr. internetového obchodu alebo dátového úložiska vo forme hostingu; pozn.

podmienkach a charakteristických znakoch služby ²¹⁴ . Pri posudzovaní obchodných postupov sa zohľadňuje znenie nasledujúceho článku;

- c) Článok 3 odst. 3 prvým a tretím odsekom obmedzuje postupy IAP pri riadení prevádzky siete, na ktoré je stanovené pravidlo rovnakého zaobchádzania so všetkým prenosom dát. Tým sú generálne zakázané praktiky, *inter alia*, blokovania, spomaľovania, obmedzenia a diskriminácie prístupu koncového užívateľa ku špecifickému obsahu alebo aplikáciám zo strany IAP. Takýto právny stav by ale významne limitoval možnosti IAP spravovať bežnú prevádzku siete ako i prípadné zásahy štátu alebo správneho orgánu. Preto je súčasne druhým odsekom pripustená možnosť IAP vykonávať „opatrenia na primerané riadenie prevádzky“ postavené na princípe transparentnosti a primeranosti a zároveň nezaložené na obchodných kritériách, ale objektívnych technických požiadavkách na kvalitu poskytovanej služby prístupu k internetu²¹⁵. Takýmito opatreniami je ďalej zakázané monitorovať špecifický obsah, ktorý koncoví užívatelia prenášajú pomocou siete²¹⁶. Tretí odsek obsahuje dva aspekty – je to jednak všeobecný zákaz prijímať opatrenia IAP, neprimerané potrebám riadenia

²¹⁴ Taktiež v zmysle čl. 4 odst. 1 písm a) až e) spoločne so zvýšenou informačnou povinnosťou poskytovateľov IAP smerom ku koncovým užívateľom sa bude sa jednať o jasné, zrozumiteľné a transparentné informácie o vplyve opatrení IAP na riadenie prevádzky, rýchlosť pripojenia pri sťahovaní, prenášaní a nahrávaní, o zjednanej cene za poskytované služby, limitáciu objemu prenášaných dát napr. cez mobilné zariadenie a funkčné nápravné prostriedky, ktoré má koncový užívateľ v pozícii spotrebiteľa k dispozícii v prípade pravidelne opakujúcej sa nezrovnalosti medzi skutočnou a proklamovanou výkonnosťou služieb prístupu k internetu, pokiaľ ide o definičné parametre služby.

²¹⁵ Tým je vymienená možnosť prijať opatrenia, ktoré hlavne optimalizujú kvalitu poskytovaných služieb a celkový dátový prenos koncových užívateľov. Obchodným kritériom sa rozumejú hlavne neprimerané poplatky spojené s obmedzením určitého typu prevádzky dátového prenosu ako napr. VoIP, viz. nižšie. Transparentnosť sa dotýka hlavne informačnej povinnosti podľa čl. 4 Nariadenia (EÚ) 2015/2120 o týchto opatreniach zmienená v referencií č.88 tohto dokumentu.

²¹⁶ Výnimku tvorí monitoring generického obsahu na dobu potrebnú k primeranému riadeniu internetovej prevádzky. Takýto obsah je štandardne obsiahnutý v prenášaných paketoch IP a protokole TCP. Bližšie kapitola 1.3

prevádzky²¹⁷ a ďalej taxatívne špecifikuje tri výnimky z generálnej klauzuly, za ktorých prijaté opatrenia poskytovateľmi internetových služieb môžu odchyliť od generálneho pravidla. To však jedine v odôvodnených prípadoch ak je to potrebné a iba na tak dlho ako je to skutočne potrebné. Tým sa významne obmedzili autoregulačné možnosti a tendenčný postup ISP pri blokovaní prístupu k závadnému obsahu, ktorý nemá k blokovaniu povolenie vyplývajúce z právneho poriadku členského štátu alebo Európskej Únie.

Výnimky z generálneho pravidla v písm. b) a c) článku 3 odsek tretí, ktorým sa súhrnne hlbšie v práci nebudeme venovať, sú určené k možnosti IAP prijať výnimočné opatrenia k zachovaniu integrity a bezpečnosti siete a služieb poskytovaných jej prostredníctvom²¹⁸ a predchádzaniu hroziacemu zaťaženiu siete alebo nediskriminačnému zmierneniu účinkov a dopadu takého výnimočného a dočasného preťaženia siete²¹⁹.

Výnimku z generálneho pravidla v písm. a) článku 3 odsek tretí, s ktorého znením budeme v práci ďalej pracovať, môže IAP využiť, aby: „*sa dodržali legislatívne akty Únie alebo vnútroštátne právne predpisy, ktoré sú v súlade s právom Únie, ktorým poskytovateľ služieb prístupu k internetu podlieha, alebo*

²¹⁷ Ako príklad by poskytovatelia internetových služieb nemali blokovať, spomaľovať, meniť, obmedzovať, narúšať alebo diskriminovať reklamu pri poskytovaní IAS, pokiaľ nie sú v konkrétnom prípade splnené podmienky jednej z taxatívnych výnimiek k takémuto opatreniu podľa článku 3 odst. 3 odsek tretí.

²¹⁸ Typickým útokom na integritu siete sú kybernetické útoky ako napríklad tzv. cieľené odoprenie služby (známe pod ang. skratkou DoS, *Denial of Service*, pozn.) alebo prístupu ku sieti treťou osobou využitím sieťovej chyby s možnosťou preťaženia siete. V týchto prípadoch môže IAP pristúpiť *ex post* napríklad k blokácii IP adries koncových užívateľov, ktorých je možno považovať za známe alebo podozrivé zdroje útoku.

²¹⁹ Recitál 15 Nariadenia (EÚ) 2015/2120 rozdeľuje preťaženie na dočasné, ku ktorému môže dochádzať pri náhlom náraste počtu užívateľov alebo dopytu po špecifickom obsahu, čím môže byť prekročená prenosová kapacita siete a ostatné služby spomalené a výnimočnom preťažení pri nepredvídateľných a neodvratných situáciách ako technická porucha infraštruktúry alebo vyplývajúce z núdzovej situácie. Po zistení príčin je na opatrení IAP či prikróčí ku blokovaniu alebo spomaleniu siete, táto výnimka nemôže mať ale stálu povahu. V takých prípadoch by mal v teórii IAP pristúpiť ku rozšíreniu kapacity siete na výzvu dozorového orgánu (napr. ČTÚ, pozn.).

opatrenia, ktoré sú v súlade s právom Únie, ktorými sa vykonávajú takéto legislatívne akty Únie alebo vnútroštátne právne predpisy, vrátane rozhodnutí súdov alebo orgánov verejnej moci s príslušnými právomocami“²²⁰. Recitál 13 túto výnimku rozvádza na situácie, v ktorých IAP podlieha napríklad normám týkajúcim sa zákonnosti obsahu, aplikácií alebo služieb najmä s ohľadom na verejnú bezpečnosť ako aj normám trestného práva, na základe ktorých môže byť vyžadované blokovanie špecifického obsahu, a to i na základe opatrení ktorými sa vykonávajú alebo uplatňujú legislatívne akty Únie alebo vnútroštátne predpisy, teda napríklad súdne rozhodnutie a rozhodnutia orgánov verejnej moci, v ktorých je vyžadovaná blokácia špecifického obsahu. Recitál 13 taktiež kladie dôraz na dodržiavanie súladu s požiadavkami vyplývajúcimi z Charty základných práv Európskej Únie. Konkrétne je invokovaný článok 52 ²²⁰, ktorý stanovuje aby akékoľvek obmedzenie práv a slobôd uznaných Chartou bolo stanovené zákonom a rešpektovalo podstatu týchto práv a slobôd. Ako vyplýva zo znenia recitálu 13 pre všeobecný záujem, uznaný Úniou, by malo byť obmedzenie zavedené len v „*prípadoch vhodných, primeraných a nevyhnutných v demokratickej spoločnosti*“²²¹;

- d) Článok 3 odst. 4 stanovuje podmienky, za ktorých opatrenia pri riadenie prevádzky siete môžu mať za následok spracovanie osobných údajov; a Článok 3 odst. 5 stanovuje slobodu IAP poskytovať špecializované služby a podmienky, za ktorých môže byť táto sloboda uplatňovaná.

²²⁰ Charta základných práv Európskej Únie (2010/C 83/02). Čl. 52: „*Akékoľvek obmedzenie výkonu práv a slobôd uznaných v tejto charte musí byť ustanovené zákonom a rešpektovať podstatu týchto práv a slobôd. Za predpokladu dodržiavania zásady proporcionality možno tieto práva a slobody obmedziť len vtedy, ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných*“.[cit. 10.3.2018]. Dostupné i online z:

eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:sk:PDF

²²¹ srov. znenie Recitál 13 Nariadenia (EÚ). 2015/2120

Uvedený výklad je právne – technického charakteru, ktorého pravidlá a limity nemusia pôsobiť na prvý pohľad zrozumiteľne. Preto sa ich pokúsime vyjasniť príkladom dnes rozšíreného využívania aplikácií „Voice-over-IP“ ako napr. Viber alebo Skype namiesto hlasovej služby na telefonovanie poskytovanej telekomunikačnými operátormi. VoIP je mechanizmus internetového prenosu s názvom „packet switching“ umožňujúci hlasové volania prostredníctvom internetu. Pri prepínaní paketov rozdelí odosielateľ údaje na malé bloky a prenáša ich cez internetovú sieť, čo je presne to, čo sa stane s hlasovými alebo obrazovými dátami odosielateľa pri používaní služby volania VoIP. Hlasové údaje sú komprimované a rozdelené na malé bloky, ktoré sa posielajú cez internet príjemcovi telefonátu na druhej strane internetu²²². Pochopiteľne v prospech využívania týchto služieb koncoví užívatelia opúšťajú trh tradičných telekomunikačných operátorov poskytujúcich hlasové volania. V tejto spojitosti využíva BEREC Guidelines pojem pod-internetové služby („sub-internet services“, pozn.)²²³, ktorú posudzuje ako službu, ktorá obmedzuje prístup ku určeným službám ako napr. využívanie mobilnej LTE siete na VoIP, alebo poskytuje prístup iba k predom určenej časti internetu. Zároveň zdôrazňuje úlohu národných regulátorov v posudzovaní zmluvných dojednaní podmienok prístupu k elektronickej sieti, ktoré môžu zahŕňať zmluvne i technicky obmedzený prístup, čím by IAP mohol priamo obchádzať alebo porušovať čl. 3 odst. 1, 2 a 3 Nariadenia (EÚ) 2015/2120. Príkladom by mohol byť veľký telekomunikačný operátor, ktorý zároveň poskytuje mobilný prístup k internetu, vedený ekonomickým záujmom zablokuje využívanie internetového pripojenia na súbor aplikácií umožňujúci VoIP. I keď je nepravdepodobné, že by užívatelia k týmto zmluvným podmienkam pristúpili, IAP by sa ich ponúkaním a následným poskytovaním dopustil priameho obmedzenia práv koncových užívateľov, čím by porušili článok 3 odst. 1. Súčasne by takáto dohoda bola neprípustná podľa čl. odst. 2 a jej plnenie by porušovalo princípy

²²² COHEN-SHEFFER Natalie. *What is VoIP?* [online]. Viber Blog, publikované 13.11.2017 [cit. 13.3.2018]. Dostupné z: www.viber.com/blog/2017-11-13/what-is-voip/

²²³ BEREC Guidelines, 2016, op.cit., s.6 marginália 17.

nediskriminačného prístupu ku všetkým aplikáciám, teda i VoIP podľa čl. 3 odst. 1 a čl. 3, v prípade že by išlo o stály stav blokovania prístupu²²⁴.

Článok 5 odst. 1 Nariadenia (EÚ) 2015/2120²²⁵ poveril správnym dozorom nad dodržiavaním článkov 3 a 4 a presadzovaním pravidiel národný regulačný orgán, v českom prostredí Český telekomunikačný úrad. Poniekaľ úzko špecifikované povinnosti pre národné regulačné orgány vyplývajúce z nariadenia 2015/2120 boli bližšie usmernené metodickými pokynmi na vykonávanie povinností národných regulačných orgánov podľa rovnakého článku, ktorých vypracovaním bol čl. 5 odst. poverené združením BEREC²²⁶ s cieľom bližšie prispieť k ich jednotnému uplatňovaniu.

4.2 Základné postoje k blokovaní prístupu k obsahu

Poznatky z tejto práca nás vedú k uvažovaniu o ISP resp. IAP, ako o technických autoritách, ktoré obmedzujú prepojitelnosť k akýmkoľvek koncovým bodom internetu len vo výnimočných prípadoch. Tým rešpektujú slobodu voľby užívateľského rozhodnutia, ku ktorým možnostiam, aplikáciám alebo službám siete pristúpia. Každá sloboda na internete však musí mať nastavené určité vonkajšie limity ako i v reálnom svete, inak by sa z kyberpriestoru pomaly stával deviantný priestor. Chápanie idealistického média oslobodeného od reštrikcií je dávno stratené spoločne s ideálmi kybernetikov deväťdesiatych rokov. V tomto zmysle je absolútnou necesitou zakotviť nielen prístup k otvorenému internetu ale aj jeho horný limit a realizáciu. Javí sa nebezpečným pomyslieť na priestor v ktorom anonymita živí kriminalitu a nenávisťný prejav bez zábran. A i keď sa objavujú

²²⁴ BEREC Guidelines, 2016, op.cit., s.11 a s.15 marginálie 38 a 55 resp.

²²⁵ Čl. 5: „Národné regulačné orgány podrobne monitorujú dodržiavanie článkov 3 a 4 a zabezpečujú súlad s nimi a podporujú nepretržitú dostupnosť nediskriminačných služieb prístupu k internetu na takých úrovniach kvality, ktoré odzrkadľujú pokroky v technológii. Na uvedené účely môžu národné regulačné orgány ukladať jednému alebo viacerým poskytovateľom elektronických komunikácií pre verejnosť vrátane poskytovateľov služieb prístupu k internetu požiadavky týkajúce sa technických charakteristík, minimálne požiadavky na kvalitu služieb a ostatné primerané a nevyhnutné opatrenia. Národné regulačné orgány každoročne uverejňujú správy o ich monitorovaní a súvisiacich zisteniach a tieto správy poskytnú Komisii a orgánu BEREC.“

hlasy, ktoré by neváhali vnímať internet dionýzovským pesimizmom, stále existujú relatívne účinné prostriedky vyplievania záhrady internetu od obsahovej buriny predtým, ako ju paraziticky pohlť.

Takýmito prostriedkami sú blokovanie, filtrovanie a prípadne iné zamedzenie prístupu k obsahu a druhotný inštrument odstránenia obsahu zo siete. Tieto pojmy by sa ale nemali výrazovo zamieňať. Vo všeobecnosti bude v súhrne blokovanie označovať hlavne technické opatrenie ISP zamerané na obmedzenie prístupu k cielenému obsahu, informáciám pomocou softwarových alebo hardwarových produktov. To sa dá dosiahnuť prostredníctvom zablokovania systému DNS (Domain Name System), IP adresy alebo nástroja Uniform Resource Locator (URL)²²⁷. Odstránenie internetového obsahu na druhej strane namiesto toho široko odkazuje na požiadavky alebo opatrenia zamerané na prevádzkovateľa služieb „hostingu“, najčastejšie dátového úložiska alebo webových stránok k odstráneniu nezákonného obsahu webových stránok²²⁸.

Z hľadiska užívateľa je zvolený pojem menej dôležitý ako účinok: niektorá časť internetu je neprístupná. Pre zákonodarcu a digitálnych aktivistov je výber konkrétneho výrazu zvyčajne motivovaný sémantickým podtónom, a nie technicky správnym použitím

²²⁷ ISP používajú na zablokovanie obsahu na internete jednu z troch techník. DNS, IP alebo hybridné blokovanie. Blokovanie DNS znamená, že poskytovatelia internetových služieb zasahujú do tabuľky DNS pod svojou kontrolou, aby zabránili tomu, aby individuálna žiadosť užívateľa dosiahla požadovanú webovú stránku. Blokovanie DNS ovplyvňuje všetky informácie a služby poskytované príslušnou doménou. Blokovanie IP zabráňuje vytváraniu spojení medzi serverom / webovou lokalitou a cieľovou adresou IP, bráni prístupu užívateľov. Obidve techniky sú ohrozené obchádzaním, ako aj nadbytočným blokovaním obsahu, ktorý nepredstavuje hrozbu. Hybridné blokovanie je kombináciou blokovania IP a DNS, ktorá je navrhnutá na riešenie problému nadmerného blokovania, avšak táto forma blokovania si vyžaduje investície do infraštruktúry na strane ISP a spôsobuje značné oneskorenie času odozvy. Hybridné blokovanie je náchylné na rovnaké obchádzania ako blokovanie DNS a IP. Výklad obsahovo prevzatý srov. EuroISPA. *Internet blocking: frequently asked questions* [online]. Europe internet services providers association, [cit. 25.3.2018]. Dostupné z: <http://www.euroispa.org/internet-blocking-frequently-asked-questions/>

²²⁸ Komparatívna štúdia SICL, 2015, op.cit., s. 12

²²⁹. Zatiaľ, čo slovo "*cenzúra*" vyvoláva nesporne negatívnu konotáciu zásahu do práv užívateľa, pod slovom "*filtrovanie*" si predstavíme jemnejšiu až neškodnú operáciu, ako odstránenie hnilých bobúľ zo strapca hrozna.

Pri dlhoročnej absencii regulačného rámca Európskej Únie nie je náhodou, že legislatívny prístup krajín EÚ ako i členmi Rady Európy je roztrieštený. Komparatívna štúdia SICL identifikovala dva myšlienkové prúdy prístupu k blokovaniam, filtrovaniu a odstraňovaniu nelegálneho internetového obsahu a na tomto základe postavila národné modely regulácie²³⁰.

4.2.1 Model krajín s nedostatočným národným regulačným rámcom

Prvým modelom sú krajiny, ktoré neprijali osobitné právne predpisy týkajúce sa blokovaniam a odstraňovania internetového obsahu porušujúcim určitú právnu normu, čo je argumentované odbornou verejnosťou ako nemožnosť zákonodarcu legislatívne sekundovať rýchlemu technologickému vývoju²³¹. Pri neexistencii systemizovanej regulácie, teda zákonom určených a cielených podmienok a postupov sa viacero krajín opiera v rozdielnej miere o „všeobecné“ právne predpisy, i keď tie často na obsah publikovaný na internete výslovne neodkazujú. Pri aplikácii teda ostáva metóda *analogia legis* pri ktorej aplikujeme právnu normu najpodobnejšiu. Problémom tejto interpretácie je stieranie špecifik regulovaného objektu – internetu resp. kyberpriestoru proti reálnemu hmotnému svetu. Medzi tieto štáty patrí k decembru 2015 napríklad Poľsko a Česká republika. Práve Česká republika nám poslúži ako príklad rastúcej konfrontácie idealistickej predstavy postačujúceho legislatívneho rámca s realitou pri sporoch súvisiacich s obsahom internetu. Môžeme tvrdiť, že práve absencia úpravy generálneho zásahu proti nelegálnemu obsahu,

²²⁹ Internet Society. *Perspectives n Internet Content Blocking: an Overview*[online]. Publikované 3/2017 [cit. 17.3.2018]. s. 5-7.

Dostupné z: cdn.prod.internetsociety.org/wp-content/uploads/2017/03/ContentBlockingOverview.pdf

²³⁰ Komparatívna štúdia SICL, 2015, op.cit., s.12

²³¹ Napríklad americký pohľad TANNEERU Manav. *Legislation can't keep pace with technology* [online]. CNN, publikované 18.10.2005 [cit. 25.3.2018]. Dostupné z: edition.cnn.com/2005/TECH/10/17/wireless.legislation/index.html

alebo jej aplikačnej skrytosti, doviedla ČR k prijatiu zásadných ustanovení v zákone č. 186/2016 Sb., o hazardných hrách, o ktorých budeme hovoriť v kapitole 4.5. Otázkou do budúcnosti ostáva, či je udržateľným stav kombinovaného mechanizmu neregulovaného rámca s núdzovými legislatívnymi zásahmi v konkrétnych sektorových oblastiach.

Pri legislatívnom vákuu, často prijíma samoregulačné opatrenia súkromný sektor prezentovaný ISP. Takýto postup je v súčasnosti podľa Nariadenia (EÚ) 2015/2120 limitovaný²³². Ako uvádza komparatívna štúdia SICL²³³, v niektorých jurisdikciách, ako napríklad v Spojenom kráľovstve je blokovanie, filtrovanie a odstránenie nelegálneho obsahu do značnej miery dosiahnuté práve pomocou koordinovanej súkromnej regulácie buď prostredníctvom politiky používania internetových sprostredkovateľských podmienok alebo dobrovoľnej spolupráce ISP s policajnými orgánmi. Úprava je sprevádzaná legislatívnymi pravidlami vo vymedzených oblastiach, ako napríklad odstránenie teroristických materiálov a upravenie zaznamenaniu a odstránenie (*notice and take-down, pozn.*) škodlivého obsahu. V iných štátoch, ako napríklad vo Švajčiarsku je opatrenie o blokácii určitého typu obsahu realizované iba po dialógu medzi príslušnými správnymi orgánmi a IAP²³⁴.

Ostatné krajiny, vychádzajúc z časti druhej - *country reports* Komparatívnej štúdie SICL, za ktoré môžeme uviesť Nemecko a Holandsko, sa spoliehajú na obecné súdy, aby zabezpečovali rovnováhu medzi slobodou prejavu a bezpečnosťou internetu na jednej strane a ochranou ostatných základných práv na strane druhej v čo najprirodzenejšej miere.

4.2.2 Model krajín s cieľným národným regulačným rámcom

Druhým modelom sú právne systémy, v ktorých zákonodarca vytvoril právny rámec, ktorého cieľom je regulovať digitálne médiá ako internet vrátane úpravy blokovania,

²³² Bližšie k limitáciám viz. kapitola 4.3

²³³ Srov. Komparatívna štúdia SICL, op.cit. stat' 1.1, s.13

²³⁴ Pokyny k postupu zaznamenaniu a odstráneniu od Swiss Internet Industry Association. *Hosting Code of Conduct. Notice and take down* [online]. swisscom, publikované 1.2.2013 [cit. 25.3.2018]. Dostupné napr. z: www.swisscom.ch/content/dam/swisscom/en/biz/sme/it-hosting/pdf/wh_verhaltenskodex-simsa_en.pdf

filtrovaní a odstraňování internetu. Takéto právní předpisy by měli stanovit právní základ, který odůvodňuje blokování nebo odstránění obsahu, súdny alebo správny orgán, ktorý môže opatrenia aplikovať a právné regulačný rámec²³⁵.

Právní základ blokování a odstraňování obsahu, na ktorom je tradične postavená odpovedajúca legislatíva tohto modelu v zásade interpretačne zodpovedá záujmom, ktoré chráni i čl. 10 odst. 2 európskeho Dohovoru o ochrane ľudských práv a základných slobôd²³⁶. I napriek obsahovej príbuznosti, štáty často pristupujú k vymedzeniu právneho základu značne kreatívne. V tejto súvislosti je právnym základom najmä ochrana²³⁷:

- a) *zdravia a morálky*, ku ktorým sa najčastejšie vzťahujú opatrenia zamerané na ochranu pred obsahom sexuálneho zneužívania detí a nezákonným online hazardom. Niektoré krajiny ako Ruská federácia vykladajú tento právní základ blokování obsahu skôr extenzívne a priradzujú sem napr. obsah s obscénnosťami, inú ako detskú pornografiu alebo tzv. homosexuálnu propagandu.
- b) *národnej bezpečnosti, územnej celistvosti alebo verejnej bezpečnosti*, ku ktorým sa vzťahujú hlavne opatrenia na blokáciu a odstránenie obsahu s teroristickou aktivitou.
- c) *povesti alebo iných práv*, kde pod právami, *inter alia*, rozumieme právo na ochranu súkromia a osobných údajov alebo práva duševného vlastníctva.

²³⁵ Srov. Komparatívna štúdia SICL, 2015, op.cit., stať 1.2, s.13 a násl.

²³⁶ Dohovor o ochrane ľudských práv a základných slobôd v znení ustanovení Protokolu č. 14 (CETS No. 194), ktorý nadobudol platnosť 1. júna 2010. čl. 10 odst. 2: „*Výkon týchto slobôd [Sloboda prejavu, pozn.], pretože zahŕňa povinnosti aj zodpovednosť, môže podliehať takým formalitám, podmienkam, obmedzeniam alebo sankciám, ktoré stanovuje zákon, a ktoré sú nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, územnej celistvosti alebo verejnej bezpečnosti, na predchádzanie nepokojom alebo zločinnosti, ochranu zdravia alebo morálky, ochranu povesti alebo práv iných, zabránenia úniku dôverných informácií alebo zachovania autority a nestrannosti súdnej moci*“

Dostupné z: https://www.echr.coe.int/Documents/Convention_SLK.pdf

²³⁷ Srov. výčet Komparatívna štúdia SICL, stať 1.2.1.1 až 1.2.1.4, s. 14 a násl.

4.3 Právne východiská v Českej republike

Česká republika je názorným príkladom prvého modelu v bode 4.2.1, podobne ako v mnohých európskych krajinách je miera cenzúry nízka, v prieskume z minulého roku ²³⁸ sa umiestnila na 23. mieste s hodnotením 9.5/10. Takýto stav bol utvrdený napríklad aj v roku 2013 schválením dokumentu *Státní politiky v elektronických komunikacích – Digitální Česko v.2.0, Cesta k digitální ekonomice*²³⁹. Dokument bol prijatý s úlohou zvýšenia potenciálu Českej republiky ako konkurencieschopného štátu na poli rozvoja moderných informačných a komunikačných technológií ako i služieb, ktoré sú ich prostredníctvom poskytované. K plneniu týchto cieľov si ČR prostredníctvom verejných orgánov stanovuje záväzky, ktoré realizuje 17-timi opatreniami. Ťažiskom tejto práce je i rozbor o slobode prístupu k internetu a jeho obsahu, k čomu je v opatrení č. 10 Digitálne Česko²⁴⁰ podnietené i Ministerstvo Průmyslu a Obchodu, teda k preferencií a „*podpore samoregulačných mechanizmov ISP, pretože by nemalo byť primárnym cieľom štátu implementovať štátnu reguláciu na akúkoľvek novú technológiu*“. Zároveň je treba vždy nazerať na slobodný prístup k internetu a jeho službám ale i z hľadiska bezpečnosti, ochrany súkromia. Možno i preto začlenila do Digitálneho Česka opatrenie 12²⁴¹, ktorým Česká republika garantuje, že: „*nebude blokovat komukoľvek prístup k internetu, prípadne prístup ku konkrétnym internetovým stránkam alebo on-line službám*“. Dokument ďalej uvádza, že internet je nepostrádateľným nástrojom pre podporu demokratických iniciatív politickej diskusie a uplatnenia slobody prejavu. Podnetom pre širšiu rozpravu o technickom obchádzaní blokováných stránok je téza, podľa

²³⁸ FRENKEL Alex. *Online Censorship: A Global Map & Ranking of Every Country's Internet Restrictions* [online]. vpnmentor.[cit. 15.3.2018]. Dostupné z: <https://www.vpnmentor.com/blog/online-censorship-country-rank/>

²³⁹ Ministerstvo průmyslu a obchodu. *Digitální Česko v. 2.0, Cesta k digitální ekonomice* [online]. Sekce digitální ekonomiky, publikované 2.4.2013 [cit. 20.3.2018]. Tlačová správa dostupná z: www.mpo.cz/dokument127530.html; Schválený dokument dostupný online z: www.mpo.cz/assets/cz/e-komunikace-a-posta/Internet/2013/4/Digi_esko_v.2.0.pdf (ďalej ako „*Digitálne Česko*“)

²⁴⁰ Digitálne Česko, 2013, op.cit., s.38

²⁴¹ *ibid.*, s.45

ktorej by príprava právnych predpisov nemala obsahovať povinnosti v internetovom prostredí nevymáhateľné alebo neaplikovateľné²⁴². Tieto garancie boli v povedomí spoločnosti významne narušené začlenením ustanovení §§ 82 a 84 a odpovedajúcich sankcií do ZoHH, na ktoré východiská a konkrétnu úpravu v súvislosti s blokovaním poukážeme v bode 4.5.2.

S určitosťou môžeme tvrdiť, že demokratická spoločnosť je postavená na zásadách slobody prejavu a práva na informácie ako sú zaručené v ČR článkom 17 Ústavného zákona č. 2/1993 Sb., Listina základních práv a svobod²⁴³. V tomto ponímaní sú hmotné a procesné záruky zabrániť neodôvodnenému obmedzeniu prístupu k obsahu ako aj primeranosti a nevyhnutnosti v demokratickej spoločnosti prijatých opatrení pozitívne zaručené ústavnou slobodou prejavu a práva vyhľadávať a šíriť informácie s možnosťou ich obmedzenia výhradne zákonom a len na základe dôvodov uvedených v LZPS čl. 17 odst. 4. Česká legislatíva, ale zákonom nedefinuje generálny postup blokovania, filtrovania ani odstraňovania nelegálneho internetového obsahu, na základe ktorých by mohli byť prijaté sektorové špeciálne zákony. Možnosťou ostáva súdne alebo správne rozhodnutie, ktorým sa uloží povinnosť príkazom a zvolené technické prostriedky sú ponechané v kompetencii ISP. Pri aplikácii opatrení môžu zo strany štátu napomáhať metodické pokyny príslušných orgánov štátnej správy (napr. Ministerstvo Financíí, Ministerstva Průmyslu a Obchodu alebo ČTÚ).

²⁴² *ibid.*, s.45

²⁴³ Článok 17 odst (1) až (4) Ústavného zákona č. 2/1993 Sb., Listina základních práv a svobod:

„(1) Svoboda projevu a právo na informace jsou zaručeny.

(2) Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu.

(3) Cenzura je nepřipustná.

(4) Svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti.“

Taktiež je nutné uviesť, že česká legislatíva zásadne nerozlišuje medzi pojmami blokovanie, filtrovanie a odstránenie obsahu. Rozhodli sme sa použiť "blokovanie" ako jednoduchý a priamy výraz. Pre úplnosť uvedme, že o blokácii obsahu môžeme hovoriť v 3 úrovniach:

- 1) Na základe zákona alebo rozhodnutia súdu alebo správneho orgánu. Ide teda o dodržanie európskych a národných zákonných požiadaviek vyplývajúcich napr. z rozhodnutia v občianskom, trestnom a správnom konaní.
- 2) Opatrenie ISP, prijaté v súvislosti s udrжанím sa vo *vodách bezpečného prístavu*, teda napr. odstránenie obsahu porušujúceho práva duševného vlastníctva. Taktiež pod túto množinu môžeme vzťahovať opatrenia prijaté IAP v rámci dobrovoľného blokovania, ku ktorým podotýkame, že v prípade nesúlady s požiadavkami Nariadenia (EÚ) 2015/2120 v nich ISP od 31. decembra 2016 nebude môcť pokračovať²⁴⁴. Ide napríklad o prípady dobrovoľného zavedenia metódy samoregulácie prevádzky elektronickej siete poskytovateľom internetového pripojenia, tzv. *blacklistingu*²⁴⁵, ktorým zabezpečí blokovanie vymedzeného zoznamu adries s nevhodným a nezákonným obsahom vedeným napríklad nezávislou *Internet Watch Foundation*²⁴⁶. V ČR k blokovaní stránok s nezákonným obsahom súvisiacim so sexuálnym zneužívaním detí pristúpila napríklad O2 Telefónica²⁴⁷. Takéto opatrenie by nemalo v teórii odporovať Nariadeniu (EÚ) 2015/2120, ako poukážeme v bode 4.4.1.

²⁴⁴ čl. 10 odst. 3. Nariadenie (EÚ) 2015/2120: „Členské štáty môžu ponechať do 31. decembra 2016 v platnosti vnútroštátne opatrenia vrátane samoregulačných mechanizmov účinné pred 29. novembrom 2015, ktoré nie sú v súlade s článkom 3 ods. 2 alebo 3.“

²⁴⁵ VYMĚTAL Petr. *Černé listiny* [online]. Pracovní text pro Ministerstvo vnitra ČR. [cit. 25.3.2018]. Dostupné z: www.mvcr.cz/soubor/studie-vymetal-blacklisting-pdf.aspx vymezil blacklist ako: „*rejstřík subjektů [adries], které nějakým způsobem nesplňují anebo porušují určitá uznaná pravidla*“.

²⁴⁶ Internet Watch Foundation. Dostupné z: <https://www.iwf.org.uk/>

²⁴⁷ MACICH Jiří. *Telefónica potvrdila filtrování stránek* [online]. Lupa.cz. Publikované 14.8.2009 [cit. 17.3.2018]. Dostupné z: <https://www.lupa.cz/clanky/telefonica-o2-potvrdila-filtrovani-stranek/>

- 3) Koncovému užívateľovi, ale napríklad aj lokálnej univerzitnej sieti je priznaná možnosť vypnutia a zapnutia blokovania webových stránok na základe vlastného rozhodnutia v reálnom čase využitím služby alebo softwaru nainštalovaného na zariadení, teda bez zásahu ISP. Typickým príkladom je využitie tzv. antivírových programov, ktoré automaticky blokujú alebo upozorňujú na škodlivý obsah a inak chránia užívateľa, ktorý sa tejto blokácií vedome a dobrovoľne podrobuje alebo rodičovského zámku k zablokovaniu prístupu k nevhodnému obsahu na internete, kde je takéto opatrenie ponechané na diskreii zodpovedného rodiča. Poskytovatelia však nemôžu ponúkať a umožňovať blokovanie určitého obsahu vo verejne dostupnej komunikačnej sieti bezdôvodne, a to ani na žiadosť koncového užívateľa. Dôvodom tohto opatrenia je skutočnosť, že práve blokovanie obsahu priamo v sieti je spôsobilé v dôsledku viesť k obchádzaniu cieľu a účelu Nariadenia (EÚ) 2015/2120²⁴⁸.

Táto úprava je na úrovni zákonov doplnená obrovským množstvom predpisov upravujúcim jednotlivé časti internetového práva napríklad prenosu obsahu a obmedzení sieti elektronických komunikácií v ZoElKom a regulácie obsahu v ZoNSIS, zákone č. 121/2000 Sb., autorský zákon, zákone č. 89/2012, občanský zákoník, úpravy bezpečnosti a integrity siete v zákone č. 181/2004 Sb. o kybernetickej bezpečnosti a trestnoprávnym rámcom, okrem ďalších použiteľných právnych predpisov.

4.4 Vybrané problémy trestnoprávneho rámca

Pri možnostiach blokovania alebo odstraňovania obsahu, musíme nutne, i keď to nie je ďalším predmetom tejto práce, v krátkosti nadviazať výkladom trestnoprávnej roviny k možnostiam uloženia povinnosti ISP zo strany súdu formou začlenenia do meritórneho rozhodnutia alebo uznesením o vydaní veci či odňatie veci v trestnom konaní. Ako sme

²⁴⁸ Srov. bližšie k obmedzovaniu prístupu k obsahu. Český Telekomunikační Úřad. *Vyjádření Českého telekomunikačního úřadu k vybraným otázkám přístupu k otevřenému internetu a evropským pravidlům síťové neutrality* [online]. Publikované 23.3.2017 [cit. 18.3.2018]. Dostupné z: www.ctu.cz/vyjadeni-ceskeho-telekomunikacniho-uradu-k-vybranim-otazkam-pristupu-k-otevrenemu-internetu. s. 3 až 4

rozobrali v časti 3, výnimky zo zodpovednosti ISP, nemajú vplyv na možnosť súdu alebo správneho orgánu vydávať príkazy rôznych druhov, ktoré môžu mať podobu rozhodnutia súdu al. správnych orgánov, ktorými sa požaduje ukončenie protiprávneho jednanie alebo predchádzať protiprávnemu jednaniu vrátane odstránenia nezákonných informácií alebo znemožnenie prístupu k nim. Tie často, ako uvedieme na teoretickom príklade, plnia dobrovoľne a často s predstihom alebo na základe výzvy policajného orgánu. K problematike aplikácie podávame bližšie vysvetlenie v poznámke pod čiarou²⁴⁹.

V trestnoprávnej rovine sa v ČR uplatňuje základné pravidlo, čo je nezákonné offline je taktiež nezákonné online. Téma počítačovej kriminality alebo aj „*cybercrime*“²⁵⁰, o ktorej sa v prostredí českých odborných kruhov teoretizuje návrhmi implementácie nových

²⁴⁹ Srov. k možnosti súdu al. správneho orgánu recitál 45 a napr. článok 12 odst. 3 smernice 2000/31/ES; K možnosti IAP nariadenie súdu realizovať taktiež čl. 3, odsek tretí, písm. a) Nariadenia (EÚ) 2015/2120. Táto možnosť však do zákona o službách informačnej spoločnosti zo smernice transponovaná nebola, neobsahuje ani odkaz na zvláštny právny predpis podľa ktorého by bolo možné postupovať. V prípade absencie je potrebné teda aplikovať teleologický výklad poukázať na judikatúru v európskych okolitých krajinách s podobnou právnou úpravou.

Prevzaté, bližšie k výkladu : POLČÁK, *Právo na internetu: spam a zodpovednosť ISP*, 2007, op.cit., s. 77

²⁵⁰ V súčasnosti si dovoľíme *desuetudo* opustiť tradičný pojem „*počítačová kriminalita*“ v prospech modernejšieho poňatia „*informačná kriminalita*“ alebo vhodnejší anglický názov „*cybercrime*“.

„*Tento typ kriminality pozostáva z trestných činov, ktoré sa spáchajú online prostredníctvom elektronických komunikačných sietí a informačných systémov. Tento problém možno rozdeliť do troch všeobecných definícií:*

1) Trestné činy špecifické pre internet, ako sú napríklad útoky na informačné systémy alebo phishing (napríklad falošné webové stránky bankových stránok na vyhľadávanie hesiel umožňujúcich prístup k bankovým účtom obetí).

2) Trestné činy využívajúce internet k ich spáchaniu ako online podvody a falšovanie. Podvody môžu byť spáchané online prostredníctvom nástrojov ako krádež identity, phishing, spam.

3) Nezákonný online obsah, vrátane materiálov týkajúcich sa sexuálneho zneužívania detí, podnecovanie k rasovej nenávisti, podnecovanie k teroristickým činom a oslave násillia, terorizmus, rasizmus a xenofóbia.

Prevzaté z: European Commission. *Cybercrime* [online]. [cit. 16.3.2018]. Dostupné z: ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

skutkových podstát už od deväťdesiatych rokov²⁵¹ je v základe označenie skupiny trestných činov vedených spoločným faktorom – počítačom, programom, dátami²⁵², ktoré závažným spôsobom zasahujú do individuálnych subjektívnych práv (právo na súkromie) a nedistributívnych verejných statkov ako solidarita či mravnosť²⁵³. K rýchlym obmenám v informačnej spoločnosti uvedieme aspoň dôležitú prvú harmonizačnú snahu na úrovni Rady Európy v Budapešti dňa 23. októbra 2001²⁵⁴, keď bola otvorená k podpisu členskými štátmi Dohoda o počítačovej kriminalite (Convention on cybercrime, Convention sur la cybercriminalité, pozn.) s úlohou stanoviť medzinárodný právny rámec pre účinné potieranie počítačovej kriminality prostredníctvom harmonizácie prvkov skutkových podstát a medzinárodnej spolupráce²⁵⁵, rozšírenou o Dodatkový protokol o kriminalizácii činov rasistickej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov.

Skutkové podstaty, ktoré páchatel môže svojou činnosťou naplniť použitím internetovej siete, a teda súdnemu alebo správne mu orgánu je priznaná možnosť nariadiť ISP odstránenie alebo zneprístupnenie škodlivého obsahu, budú mať z povahy veci vždy formu určitého prejavu, ktorý smeruje proti základným hodnotám, ktoré demokratický štát chráni. Základným vodítkom pre možnosť spáchania trestného činu prostredníctvom počítačovej siete, a teda v rámci trestného stíhania obvineného by sme mohli pripustiť úvahu o uložení povinnosti subjektom ISP, je samotné výkladové ustanovenie zákona č. 40/2009 Sb., trestní

²⁵¹ SMEJKAL, Vladimír. Počítačová a internetová kriminalita v Českej republike. *Právní rozhledy*. 1999, roč. 1999, č. 12, s. 1 - 24. ISSN 1210-6410. s.12

²⁵² SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň : Aleš Čeněk, 2015, 636 s. ISBN 9788073805012. s.19. Takýto termín považujeme v právnej teórii trestného práva za formálne nevhodný, nie je typickým klasifikovať skupinu TČ podľa zvolených prostriedkov, o počítači a prenesene sieti je treba uvažovať ako o nástroji v rukách páchatel'a.

²⁵³ GRIVNA Tomáš, POLČÁK Radim et al. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 9788090378674. s.25

²⁵⁴ I keď sa v Českej republike stal účinnou s 12 ročným oneskorením, až dňa 1. decembra 2013 ako uvádza Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě č. 104/2013 Sb.m.s. [cit. 16.3.018]. Dostupné napr. z: <https://esipa.cz/sbirka/sbsrv.dll/sb?DR=SB&CP=2013m104>

²⁵⁵ BAYEROVÁ, Monika. Evropská úmluva o počítačové kriminalitě a sexuální zneužívání dětí. *Trestněprávní revue*, Praha: C.H.Beck, 2003, Roč. 2, č. 5, s. 156-157. ISSN 1213-5313

zákoník, o verejnom spáchaní trestného činu v § 117 písm. a): „*Trestný čin je spáchán veřejně, jestliže je spáchán ... veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem ...*“. I keď uloženie povinnosti ISP na odstránenie obsahu je v meritórnom rozhodnutí súdu zásadne možné, nejasnosť nastáva pri zabezpečení stavu počas trestného stíhania obvineného. Krátkym rozborom problematiky z pohľadu zákona č. 141/1961 Sb., trestní řád, dospejeme k poznaniu, že ustanoveniam špecificky upravujúcim počítačové dáta, nie je zo strany trestnoprávných odborníkov venovaná osobitná pozornosť. O uložení povinnosti ISP teda uvažujme skôr v kontexte existujúcich inštitútov TŘ. Takýto postup pripúšťa i doktrínálny výklad obecnej možnosti použitia analógie v trestnom práve procesnom s výnimkou zásahu do ústavne zaručených práv a slobôd²⁵⁶ ako i zaistenie súčinnosti fyzických a právnických osôb pri dožiadaní orgánov činných v trestnom konaní v zmysle § 8 TŘ²⁵⁷. Automatická úvaha nás zavedie k inštitútu predbežného opatrenia v zmysle § 88b TŘ, ale i v prípade splnenia ostatných podmienok napr. ochrana verejného záujmu môže byť týmto opatrením častovaný jedine obvinený. ISP, ako zúčastnená osoba, teda môže byť jedine adresátom edičnej povinnosti napr. rozhodnutím o zaistení veci pre dôkazné účely v zmysle § 78 TŘ: „*kdo má u sebe věc důležitou pro trestní řízení, je povinen ji na vyzvání předložit soudu, státnímu zástupci nebo policejnímu orgánu; je-li nutno pro účely trestního řízení zajistit, je povinen věc na vyzvání těmto orgánům vydat*“, i to sa však môže vzhľadom k imateriálnosti, latentnosti a nízkej životnosti digitálneho obsahu²⁵⁸ javiť enormnou požiadavkou. V krátkosti tiež podotkneme povinnosť subjektov ISP v definícii zákona o ElKom uchovávať lokalizačné a prevádzkové údaje užívateľa, ktoré sú vytvárané alebo spracované pri zaisťovaní ich verejných komunikačných sietí a poskytovaní služieb. Tieto dáta sú v súhrne podľa § 97 odst. 3) písm. a) ElKom povinní na požiadanie poskytnúť orgánom činným v trestnom konaní. V súvislosti s trestným konaním to ale nerieši samotné

²⁵⁶ JELÍNEK J. et al. *Trestní právo procesní*. 4. vyd. Praha: Leges, 2016, 848 s. ISBN 9788075021601. s.68

²⁵⁷ JELÍNEK J. et al. *Trestní zákon a trestní řád s poznámkami a judikaturou*. 7. vyd. Praha: Leges, 2017, 1312 s. ISBN 9788075022301. s. 600

²⁵⁸ GRÍVNA, POLČÁK et al., 2008, op.cit., s.130

zablokovanie prístupu k potenciálne škodlivému obsahu v dobe do vydania meritorného rozhodnutia súdu v trestnom konaní.

Je nutné uviesť, že v praxi to v tejto súvislosti nie je súdmi využívaný právny inštitút, keďže pred samotnou realizáciou rozhodnutia ISP škodlivý obsah blokujú alebo zneprístupnia po vyrozumení alebo zaistení dôkazov orgánmi činnými v trestnom konaní samostatne a často i pred, čo prispieva k obtiažnosti postihovania niektorých typov kyberkriminality. To môžeme generálne prisúdiť prirodzenej vôli ISP poskytujúcich napr. služby *hosting* neopúšťať bezpečný prístav vzhľadom k podmienke uloženej § 5 odst. 1) písm b) Zákona o NSIS²⁵⁹.

4.4.1 Spoločný boj proti sexuálnemu zneužívaniu detí na internete

Internet vďaka technickým možnostiam anonymného zdieľania obsahu či komunikácie so sebou priniesol dramatický nárast rozširovania detskej pornografie, čoho odrazom je osobitná pozornosť Európskej Únie v rámci postihovania kyberkriminality v ktorej sa problematike komerčného sexuálneho zneužívania a vykorisťovania detí venuje napr. smernica 2011/92/EÚ o boji proti sexuálnemu zneužívaniu detí²⁶⁰. Z pohľadu blokácie obsahu je najdôležitejší článok 21 a 25²⁶¹, ktoré zaväzujú členské štáty k monitoringu šírenia

²⁵⁹ ZoNSIS § 5) odst. 1 písm b: „Poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem, odpovídá za obsah informací uložených na žádost uživatele, jen ... dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo zneprístupnění takovýchto informací“.

²⁶⁰ Smernica Európskeho Parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV. Články viz. odkaz 119.

²⁶¹ Článok 21: „Opatrenia proti propagácii príležitostí na zneužívanie a sexuálnej turistiky zameranej na deti Členské štáty prijímú vhodné opatrenia na prevenciu alebo zákaz: a) šírenia materiálu propagujúceho príležitosť spáchať niektorý z trestných činov uvedených v článkoch 3 až 6 a b) organizácie ciest pre iné osoby, či už na komerčné účely, alebo nie, s cieľom spáchať niektorý z trestných činov uvedených v článkoch 3 až 5“.

Článok 25: „Opatrenia proti webovým stránkam obsahujúcim alebo šíriacim detskú pornografiu

detskej pornografie po elektronických sieťach, rovnako ako stanoviť účinné postupy v boji proti všetkým formám online zneužívania a vykorisťovania detí hlavne zakotvením postupu odstránenia stránok s týmto obsahom prevádzkovaným na ich území. Smernica umožňuje i zablokovanie prístupu k takému obsahu napr. súdnym rozhodnutím, čo nemusí byť vzhľadom k rôznym technologickým možnostiam obchádzania obmedzení dostačujúcim prostriedkom. Zabránením prístupu tzv. náhodným návštevníkom sa ale nerieši podstata problému, ako vystihujúco uviedla zástupkyňa výboru pre slobodu žien Marina Yannakoudakis: „*hlavným cieľom je odstrániť tieto stránky, pokiaľ to je možné blokovaním by malo byť doplňujúcim nástrojom*“²⁶².

Požiadavky smernice boli v prevažnej miere zapracované do TZ²⁶³ avšak je alarmujúcim, ako uvádza český europoslanec Tomáš Zdechovský, že: „*väčšina členských štátov, vrátane Českej Republiky, doposiaľ nezaviedla všetky opatrenia unijnej legislatívy, ktoré sa na prevenciu a potierania zneužívania detí zameriava*“²⁶⁴. Ide hlavne o zavedenie požiadaviek čl. 25 Smernice prijatím opatrení o odstránení resp. blokování obsahu. Forma opatrenia sa neobmedzuje na právny predpis, preto pre skutočne efektívnu realizáciu opatrení má zásadný význam zapojenie multištrukturálnej spolupráce medzi súkromným sektorom,

1. Členské štáty prijímú opatrenia potrebné na dosiahnutie toho, aby sa zabezpečilo odstránenie webových lokalít obsahujúcich alebo šíriacich detskú pornografiu, ktoré sa nachádzajú na ich území, a budú sa snažiť o zabezpečenie odstránenia takýchto stránok, ktoré sa nachádzajú mimo ich územia.

2. Členské štáty môžu prijať opatrenia na dosiahnutie zablokovania prístupu na webové lokality obsahujúce alebo šíriace detskú pornografiu používateľom internetu na ich území. Tieto opatrenia sa musia ustanoviť transparentnými postupmi a musia poskytovať primerané záruky, ktorými sa zabezpečí predovšetkým to, aby obmedzenie malo len nevyhnutný a primeraný rozsah a aby boli používatelia oboznámení s dôvodom tohto obmedzenia. Medzi tieto záruky patrí aj možnosť súdnej nápravy.“

²⁶² Európsky Parlament. *EP v boji proti sexuálnemu zneužívaniu detí* [online]. Publikované 30.9.2010 [cit. 17.3.2018]. Dostupné z: europarl.europa.eu/news/cs/headlines/society/20100927STO83658/ep-v-boji-proti-sexualnimu-zneuzivani-deti

²⁶³ Srov. §419a TZ

²⁶⁴ ČTK. *EU si došlápně na sexuálnímu zneužívání a vykořisťování dětí* [online]. tyden.cz, publikované 14.12.2017 [cit. 17.3.2018]. Dostupné z: www.tyden.cz/rubriky/zahranici/evropa/eu-si-doslapne-na-sexualnimu-zneuzivani-a-vykoristovani-deti_458989.html?showTab=diskutovane

občianskou iniciatívou a verejnými orgánmi vrátane donucovacích orgánov a súdnictva²⁶⁵. Kostra zaistenia spolupráce fyzických osôb je položená na báze dobrovoľnosti spojenou s povinnosťou vyplývajúcou z §5 Zákona o NSIS²⁶⁶ pre poskytovateľa informačnej služieb *hosting*, čím sa vytvára unifikovaný postup rôzne zapojených subjektov k zaznamenaniu a odstráneniu obsahu (*notice and take down*, pozn.). Jedná sa o nastavenie právneho mechanizmu, ktorý riadia zainteresované strany so zameraním na identifikáciu nezákonných informácií spravovaných na sieti alebo v informačnej službe a zodpovednostné zaistenie ich rýchleho odstránenia. Účinným príkladom je projekt správcu českej domén CZ.NIC pod názvom STOPonline.cz²⁶⁷, pomocou ktorého verejnosť môže nahlasovať nezákonný obsah šíriaci detskú pornografiu. Nahlasený obsah vyhodnocujú analytici z Národného bezpečnostného tímu CSIRT.CZ a potenciálne nezákonný obsah šíriaci detskú pornografiu na základe memoranda o spolupráci²⁶⁸ postúpia policajnému orgánu ČR a medzinárodnej asociácii INHOPE²⁶⁹. Poskytovateľ služby *hostingu* je informovaný po tom ako policajný orgán zaistí potrebné dôkazné prostriedky pre prebiehajúce vyšetrovanie a odsúhlasí, že

²⁶⁵ Srov. výklad možností prijatia opatrení a spolupráce v práve členských štátoch z *Report from the Commission to the European Parliament and the Council assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography* [online]. Publikované 16.12.2016 pod COM(2016) 872 final [cit. 17.3.2018]. Dostupné z:

https://ec.europa.eu/homeaffairs/sites/homeaffairs/files/20161216_report_article25_assessing_implementation_sexual_abuse_child_pornography.pdf. s.4

²⁶⁶ Čl. 14 Smernice o e-obchode

²⁶⁷ Dostupné online z: <https://www.stoponline.cz/stoponline/>

²⁶⁸ *Společná deklarace o spolupráci v rámci provozu linky pro hlášení nezákonného obsahu* [online]. [cit. 18.3.2018]. Dostupné z: https://www.nic.cz/files/nic/doc/NCOZ-20170215-deklarace_Internet-Hotline.pdf

²⁶⁹ „Medzinárodná asociácia INHOPE je celosvetovo veľmi významná asociácia bola založená v roku 1995 a od tej doby sa zaoberá bojom s obsahom zobrazujúcim sexuálne zneužívanie detí. INHOPE združuje 51 (nahlasovacích, pozn.) liniek v 45 krajinách sveta a jej hlavným cieľom je urýchliť výmenu informácií o obsahu akokoľvek zobrazujúcim sexuálne zneužívanie detí. Združenie CZ.NIC sa stalo dočasným členom tejto asociácie v júni tohto roku (2017, pozn.)“. Citované z: Blog.CZ.NIC. *STOPonline.cz v detailech* [online]. Publikované 29.11.2017 [cit. 17.3.2018]. Dostupné z: <https://blog.nic.cz/2017/11/29/stoponline-cz-v-detailech/>

obsah môže byť odstránený. Ako sme uviedli, § 5 zákona o NSIS výslovne nevyžaduje, aby ISP vyhovel požiadavkám policajného orgánu k odstráneniu obsahu, spoluprácou ISP zabezpečujú udržanie sa v režime bezpečného prístavu a zároveň vylučujú možnosť vlastného trestného stíhania ako spolupáchateľa.

4.5 Vybrané problémy správneho rámca

Pod tento rámec spadá i rozsiahla téma ochrany pred neoprávneným zasahovaním do súkromného a osobného života zverejňovaním alebo iným zneužívaním osobných údajov ako i šírenie a obsahu nevyžiadaných obchodných zdieľaní a činnosť *Úřadu pro ochranu osobních údajů*, ktorej sa bližšie venovať v tejto práci nebudeme.

Naproti tomu objasníme základy rozsiahlej diskusie ohľadne aktuálnej problematiky blokovania prístupu k určitým stránkam, ktoré sa objavujú v Českej republike v súvislosti s prijatím zákona č. 186/2016 Sb., o hazardných hrách, ktorý sa stal účinným v plnom rozsahu k 1. januáru 2017.

Ide o cnostný a zodpovedný počin modernizácie sektorovej regulácie hazardu, k prijatiu ktorej, ako uvádza dôvodová správa²⁷⁰, bol zákonodarca motivovaný dvoma ťažiskovými faktormi, a to jednak vysokými spoločenskými nákladmi na hazardné hranie a tiež rapidným rozvojom využitia moderných informačných technológií v hazarde, ktorým doterajšia právna úprava nemohla *pro futuro* postačovať. Medzi hlavné ciele novej právnej úpravy bolo výsostnou nutnosťou zahrnúť i, *inter alia*, úpravu prevádzkovania hazardných hier prostredníctvom internetu a zavedenie efektívneho kontrolného mechanizmu²⁷¹.

Dôvodová správa k ZoHH vyčerpávajúco pojednáva o variantoch prístupu zákonodarcu k novej regulácii hazardu, z ktorých odôvodnene volí najvhodnejšie riešenie oblastí, ktorým zákon venuje osobitú pozornosť. Svoje závery z hľadiska celospoločenského a právneho dopadu odvodzuje v samotnom zákone predkladateľ, Ministerstvo financií ČR (aj

²⁷⁰ Důvodová zpráva k zákonu č. 186/2016 Sb., o hazardních hrách. Sněmovní tisk č. 578/0, Poslanecká sněmovna, 7. volební období. Dostupné online z: <http://www.psp.cz/sqw/text/tiskt.sqw?O=7&CT=578&CT1=0> (ďalej ako „Důvodová správa k ZoHH“). s. 54

²⁷¹ *ibid* s.65

ako „MFČR“, pozn.) i na základe analýzy Národného ústavu duševného zdravia²⁷², ktorú nechalo MFČR pre tieto potreby vypracovať, čím umožnilo širšej verejnosti nahliadnuť bližšie do problému redukcie závislostí na hraní v záujme ochrany verejného zdravia. Už po základnom prečítaní zákona o hazardných hrách môžeme tvrdiť, že tento počin dôkladným a právne moderným spôsobom upravuje napr. druhy hazardných hier, podmienky ich prevádzkovania, opatrenia pre zodpovedné hranie a stanovuje pôsobnosť správnych orgánov v tejto oblasti.

V rámci prístupu k obsahu, je zákon o hazardných hrách i prvou sektorovou reguláciou, ktorá s určitou nadnesenosťou postavila chýbajúci základný kameň úpravy prístupu k blokovaniu obsahu na internete v Českej republike. Učinila tak po vzore niektorých členských štátov EÚ stanovením nových povinností poskytovateľom internetového pripojenia v súvislosti s blokáciou nepovolených internetových hier v ust. § 82 v spojení s § 84 zákona o hazardných hrách, ktoré špecifikuje metodickými pokynmi k plneniu tejto povinnosti²⁷³.

Celá problematika neostala bez povšimnutia českej odbornej i neodbornej verejnosti. Pomerne jednoduché znenie ustanovení ďaleko presiahla ich negatívna implikácia občianskej spoločnosti, ktorá ich prevažne razantne zvolenou sémantikou odsúdila ako chiméru cenzúry internetu. Do čela odporcov akejkolvek cenzúry internetu sa postavila napr. Pirátska strana, ktorá má nemalú podporu medzi voličmi, o čom svedčí zisk 22 „kresiel“ v Poslaneckej snemovni Parlamentu Českej republiky vo voľbách z roku 2017²⁷⁴. Predseda strany, Ivan Bartoš, sa často od prvých návrhov tohto zákona kriticky vyjadruje

²⁷² WINKLER Petr et al. *Problémové hráčství Společenské náklady na hazardní hraní v České republice*. 1.vyd. Národní ústav duševního zdraví, 2015, 98 s. ISBN 9788087142264

²⁷³ Ministerstvo Financí. *Metodický pokyn odboru 34 - Státní dozor nad hazardními hrami k plnění povinností ve věci seznamu nepovolených internetových her*) [online]. Publikované 15.1.2017 pod č. j.: MF-30513/2016/3402-14 [cit. 18.3.2018]. Dostupné z: www.mfcr.cz/cs/legislativa/metodiky/2017/metodicky-pokyn-k-plneni-povinnosti-ve-v-27269 (ďalej ako „Metodické pokyny odboru 34“)

²⁷⁴ Napr. ČTK. *Výsledky voleb: Triumf ANO, fiasko ČSSD, slaví SPD i Piráti* [online]. ceskenoviny, publikované 22.10.2017 [cit. 19.3.2018]. Dostupné z: www.ceskenoviny.cz/zpravy/vysledky-voleb-triumf-ano-fiasko-cssd-slavi-spd-i-pirati-on-line/1540980

k ustanoveniam o blokácií prístupu k internetovému obsahu, napríklad i spustením petície „Internet bez cenzúry“²⁷⁵. Argumentácia je zvolená hlavne z pohľadu zaručenia práva občanov na slobodný prejav a prístup k informáciám a prístup k sieti bez (nevyhnutnej) štátnej cenzúry. Zodpovednosť za obsah by mala byť prenesená na jeho tvorca, nie na subjekt, ktorý dáta prenáša. Šírenie a prijímanie informácií nesmie byť zákonom obmedzené. Takúto argumentáciu považujem za účelový výsek problematiky, ktorý v kontexte ochrany základných ľudských práv nepovoľuje ani teoretickú úvahu o službe spoločnosti alebo ochrane iných základných hodnôt demokratického štátu ako verejného zdravia.

Vzhľadom k dikcii ZoHH sa viac primerane javí argumentácia, Miroslava Kalouska, poslanca politickej strany TOP 09, ktorý uvádza „*Sněmovna schválila cenzuru internetu úředníkem MFČR. Byli jsme proti. Souhlas bychom nevysvětlili ani svým dětem, natož voličům.*“²⁷⁶. Ako poukážeme v bode 4.5.2 v znení ZoHH ku 1. januáru 2017 je práve Ministerstvo financií z úradnej moci rozhodujúcim orgánom o zápise na zavedený inštitút zoznamu internetových adries na ktorých je prevádzkovaná hazardná hra v rozpore so zákonom. Pri tomto spôsobe netreba opomenúť možnosť prevádzkovateľa hazardu sa proti správne rozhodnutiu účinne brániť v režime správneho poriadku, prípadne v správnom súdnictve v rámci konania o žalobe proti rozhodnutiu správneho orgánu v zmysle ust. § 65 a nasl. SŘS.

Varovne pôsobia vyjadrenia CZ.NIC ako správcu národnej domény a prevádzkovateľa *Národního bezpečnostního týmu CSIRT.CZ* podľa zákona o kybernetickej bezpečnosti, ktorý v tejto súvislosti prirovnáva postavenie MFČR k ruskému výsostnému cenzúrnemu úradu *Roskomnadzor* a vhodne sa zasadzuje o variantu rozhodovania o blokácií v súdnom konaní²⁷⁷.

²⁷⁵ Dostupné online z: www.internetbezczury.cz/

²⁷⁶ CHLUBNÁ Tereza. *Zákon o hazardu prošel sněmovnou. Opozici vadí údajná cenzura internetu* [online]. iRozhlas, publikované 13.4.2016 [cit. 19.3.2018]. Dostupné z: https://www.irozhlaz.cz/zpravy-domov/zakon-o-hazardu-prosel-snemovnou-opozici-vadi-udajna-cenzura-internetu_201604131525_dbernardy

²⁷⁷ PRŮŠA Jiří. *Blokování hazardních webů nemá v České republice i Evropě oporu ani obdobu* [online]. CZ.NIC, publikované 29.3.2016 [cit. 20.3.2018]. Dostupné z: blog.nic.cz/2016/03/29/blokovani-hazardnich-webu-nema-v-ceske-republice-i-evrope-oporu-ani-obdobu/

Usudzujeme, že prijatie zákona bolo v tejto problematike primárne vedené voľbou vhodného odôvodnenia regulačného rámca, reakčnej rýchlosti správneho orgánu na rapidný nárast nelegálnych internetových hier pri čo najmensej fiškálnej záťaži štátneho rozpočtu a výberom účelového rozhodujúceho orgánu. V nasledujúcom bode 4.5.1 preto nazrieme kritickou optikou na možné východiská zákonodarcu pri zakotvení regulácie blokovania prístupu k určitému obsahu na internete a poskytnuté odôvodnenie prijatej úpravy.

4.5.1 Možnosti regulácie nelegálneho hazardného hrania na internete

K pojednaniu o celosvetovom probléme vplyvu hazardného hrania na spoločnosť²⁷⁸ krátko odkážeme na závery analýzy problémového hráčstva vypracovanej Národným ústavom duševného zdravia ČR, ktoré ako základný pilier volí i dôvodová správa k ZoHH. Pre účely tejto práce si stanovíme teoretickú premisu – hranie hazardných hier predstavuje potenciálne ohrozenie verejného zdravia, poriadku a bezpečnosti.

MFČR v súvislosti s obsahom tejto kapitoly poukazuje na obtiažnosť dosiahnutia konsenzu a to i v rámci harmonizačného úsilia Európskej Únie s ohľadom na odlišnosť právnych úprav vo veciach ako²⁷⁹: „*verejný záujem konkrétneho štátu, bezpečnosť, kultúrne a sociálne záujmy*“. Ďalej ako hlavné právne problémy uvádza: „*otázku jurisdikcie a výkonu rozhodnutí českých orgánov voči prevádzkovateľom usadeným mimo územia Českej republiky*“. Pri prístupe k internetovej hazardnej hre očakáva hráč taktiež určitú mieru anonymity²⁸⁰, ktorá sa aplikuje i na prevádzkovateľov hazardnej hry, ktorý môžu týmto spôsobom potenciálne zastierať pôvod finančných tokov alebo inak legalizovať výnosy z trestnej činnosti. Podľa doterajšej právnej úpravy zahraničných nezákonných prevádzkovateľov by bolo v rámci správneho konania postihovať neprimerane náročné. Metodické pokyny odboru 34 taktiež uvádzajú, že okrem stanovenia prísnych podmienok pre legálnych prevádzkovateľov hazardného hrania je nutné odstrániť nelegálne možnosti hrania,

²⁷⁸ Myslíme tým hlavne negatívne dopady patologického hráčstva plynúce z hazardného hrania, pozn.

²⁷⁹ Důvodová zpráva k zákonu č. 186/2016 Sb., o hazardních hrách, op.cit., s.102

²⁸⁰ Ako uvádzajú Metodické pokyny odboru 34, možnosť anonymity môže byť využívaná osobami mladšími ako 18 rokov, ktorým sa stanovuje absolútny zákaz hry.

bez čoho nemôže byť účel a cieľ ZoHH splnený. Cieľom teda je i otvorenie českého trhu prevádzkovania hazardných hier na internete ostatným členským štátom Európskej únie.

Vytýčené paragrafy 82 a 84 ZoHH sa teda dotýkajú iba regulácie nezákonného resp. nepovoleného prevádzkovania hazardných hier prostredníctvom siete internet. Navrhovateľ zákona poukazuje na reguláciu z hľadiska predmetu regulácie kde podsadzuje varianty blokácie platby a blokáciu internetového pripojenia ku ktorej pripúšťa možnosti regulácie v správnom konaní, súdnym zákazom alebo opatrením obecnej povahy²⁸¹.

Ako sme poukázali, predkladateľ zákona pamätá i na skutočnosť, že blokácia prístupu k internetovým stránkam nemôže byť izolovaným nástrojom vymáhania²⁸², pre jeho relatívnu možnosť ľahkého obchádzania napr. proxy serverom alebo prístupom cez TOR²⁸³. Následne uvádza, že využitím týchto prostriedkov, môžeme u užívateľa prezumpovať určitý zámer obchádzať právne predpisy. Domnievame sa, že tento záver nie je dostatočne odôvodnený, nakoľko zbežný prehľad odborných sektorových článkov pre pokročilých užívateľov internetu, v dobe intruzívnych reklám a domnelého sledovania poskytovateľmi služieb svetových sociálnych sietí, odporúča rôzne metódy ako čo najúčinnnejšie chrániť svoju anonymitu a súkromie napríklad skrytím IP adresy alebo histórie prehliadania využitím anonymných prehliadačov ako TOR, a to bez zjavného zámeru obchádzať právne predpisy.

Z opačného pohľadu správca národnej domény CZ.NIC vo výzve poslancom²⁸⁴ rovnako inverzne od zákonodarcu upozorňuje na jednoduché obchádzanie blokovania stránok legálnou cestou²⁸⁵ napr. použitím technických prostriedkov zmeny DNS alebo využitia virtuálnej privátnej siete (VPN, pozn.), ktorou užívateľ simuluje prístup k internetovým stránkam z inej jurisdikcie. Treba dodať, že podobný prístup môžu zvoliť i samotní prevádzkovatelia týchto internetových stránok vytvorením systému technického

²⁸¹ Důvodová zpráva k zákonu č. 186/2016 Sb., o hazardních hrách, op.cit., s.105

²⁸² Důvodová zpráva k zákonu č. 186/2016 Sb., o hazardních hrách, op.cit., s.107

²⁸³ Domnievam sa, že zákonodarca zamýšľal uviesť pojem blokaci „obejit“ oproti „provést“ vzhľadom na ďalší výklad textu.

²⁸⁴ CZ.NIC. *Vyjádření nesouhlasu k blokování Internetu v rámci zákona o hazardních hrách* [online]. [cit. 20.3.2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Dopis_blokovani_Internetu-poslanci.pdf

²⁸⁵ Návodů možností legálního obchádzania voľne dostupné online napr. <https://www.jakobejitblokaci.cz/>

presmerovania adresy, okamžikom jej zaradenia na *blacklist*. Pri blokácií prístupu môže byť zabránené prístupu i k nezávadným stránkam, ktoré využívajú rovnakú doménu alebo IP adresu, čím by mohla byť potenciálne obmedzené povinnosti vyplývajúce pre ČR z Nariadenia (EÚ) 2015/2120, ako i porušenie ústavne zaručenej slobody prejavu.

Otázkou na regulačný rámec ostáva, prečo zákonodarca pristúpil k tejto právnej úprave primárne v súvislosti s hazardnými hrami. V súčasnej právnej úprave nie je priamo zavedený tento inštitút ani vo vzťahu k závažným trestným činom ako šírenie detskej pornografie a obdobným skutkovým podstatám trestných činov, ktoré sú ponechané na súdnom rozhodnutí alebo výzve policajného orgánu a odpovedajúcej implementácií rozhodnutia samotným ISP.

4.5.1.1 Správne konanie

Prvou z predkladaných variant blokácie konkrétneho prevádzkovateľa nelegálnych hazardných hier vládneho návrhu zákona je využitím pôsobnosti ČTÚ, ktorý vykonáva dohľad nad oblasťou elektronických komunikácií invokáciou ust. § 35 odst. 2. a 3 zákona o elektronických komunikáciách. Týmto ustanovením môže ČTÚ uložiť podnikateľovi zaisťujúcemu verejnú komunikačnú sieť²⁸⁶ alebo poskytujúcemu službu elektronických komunikácií²⁸⁷ povinnosť informovať užívateľa o cene za volania na čísla určené pre služby s vyjadrenou cenou a to i bezplatnou cestou automatického hlasového odkazu pred

²⁸⁶ Ust. § 2 písm. j) zákona o elektronických komunikáciách: „*veřejnou komunikační sítí sítí elektronických komunikací, která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací a která podporuje přenos informací mezi koncovými body sítě, nebo sítí elektronických komunikací, jejímž prostřednictvím je poskytovaná služba šíření rozhlasového a televizního vysílání*“

²⁸⁷ Ust. § 2 písm. n) zákona o elektronických komunikáciách: „*službou elektronických komunikací služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize, s výjimkou služeb, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaným službami elektronických komunikací; nezahrnuje služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací*“

poskytnutím takej služby. ČTÚ môže ďalej uložiť ISP, na základe podnetu orgánu verejnej moci príslušného k prejednávaniu podvodného konania povinnosť zablokovať prístup k takým číslam a službám, na ktorých je informačná povinnosť porušovaná, prípadne sú využívané na podvodnú činnosť. ČTÚ, ale výkladom ust. § 2 písm. n) nemá v tejto súvislosti oprávnenie regulovať resp. posudzovať samotný obsah služby. Predkladateľ zákona navrhuje MFČR ako vecne príslušný rozhodovací orgán o nelegálnosti obsahu internetových stránok, teda výslovné posúdenie obsahu služby ako nelegálnej hazardnej hry podľa ZoHH²⁸⁸. K takémuto rozhodnutiu dochádza v riadnom dvojstupňovom správnom konaní, v ktorom je zachovaný špecifický riadny opravný prostriedok rozkladu s možnosťou podania žaloby proti rozhodnutiu správneho orgánu podľa § 65 a násl. SŘS. Na základe tohto správneho rozhodnutia by následne ČTÚ vydal rozhodnutie v správnom konaní s povinnosťou ISP zablokovať prístup k internetovým stránkam, ktorých obsahom je prevádzkovanie nezákonnej hazardnej hry. Na mieste je otázka výkladu samotnej právomoci ČTÚ regulovať prístup k internetovým stránkam, na ktoré by sa podľa ZoElKom najpravdepodobnejšie vzťahla iba obmedzene na podvodné hry založené na volania na čísla, v ktorých by chýbala informácia o cene prístupu k tejto službe.

Môžeme sa domnievať, že i táto ťažkopádnosť primäla zákonodarcu pristúpiť k jednoduchšiemu a účinnejšiemu riešeniu v rámci správneho konania. ZoHH stanoví všeobecná povinnosť ISP blokovat' internetové stránky prevádzkujúce nelegálne hazardné hry, kde je o nelegálnosti obsahu rozhodované v správnom konaní Ministerstvom financií ČR, ktoré následne svoje pozitívne rozhodnutie uverejní v tzv. *blackliste*, zozname nelegálnych internetových hazardných hier. U ISP, ako osobe, ktorá je správnym aktom dotknutá, predpokladá sa súčinnosť v súlade s princípmi verejnej správy²⁸⁹. Povinnosť zamedzenia prístupu uloženú na základe zákona splnia stálym monitoringom tohto zoznamu a následného zablokovania prístupu k stránkam na ňom uvedenom. Realizáciu môžeme

²⁸⁸ Důvodová zpráva k zákonu č. 186/2016 Sb., o hazardních hrách, op.cit., s.108

²⁸⁹ Vychádzame z Odporúčania Výboru ministrov Rady Európy CM/Rec(2007)7 pre ministrov členských štátov z 20. júna 2007 o dobrej správe. POMAHÁČ, 2013, op.cit., s.169

hodnotiť ako efektívnu a účinnú s čo najmenším zaťažením štátneho rozpočtu, avšak nedostatok judikatúry v tejto oblasti činí túto predpoveď mierne odvážnou.

4.5.1.2 Súdne konanie

Ako sme uviedli v kapitole 4.1, regulácia obsahu sa môže veľmi jednoducho dostať do kolízie so základnými ľudskými právami. Práve preto predkladateľ zákona uvažil i možnosť súdneho rozhodnutia, ktoré by obsahovalo priame uloženie povinnosti ISP blokovať prístup k stránkam porušujúcim ZoHH. Ako sme pozorovali v genéze trestnoprávnej úpravy, pre potreby blokácie prístupu k obsahu sa môže súdne konanie javiť ako časovo náročné, čo môže byť zmiernené využitím predbežných opatrení²⁹⁰. I pri tejto variante vzniká možnosť rozhodnutia o *blacklistingu*, kde by o nelegálnosti obsahu rozhodoval výlučne súd a ISP by tento zoznam realizoval na základe všeobecnej povinnosti zamedziť prístup k nelegálnym internetovým stránkam ustanovenej ZoHH. I cez jeho časovú a finančnú nákladnosť sa takýto postup javí ako zaručenejšia ochrana základných ľudských práv, možnosť, ku ktorej sa prikláňali pred prijatím poslanci politickej strany TOP 09 a správca českej národnej domény CZ.NIC.

4.5.1.3 Opatrenie obecnej povahy

Opatrenie obecnej povahy ako právne záväzný konkrétny abstraktný správny akt je forma správnej činnosti, ktorý nie je právnym predpisom ani rozhodnutím²⁹¹, vydané podľa § 171 SŘ na základe zvláštného zákona. Konkrétnosť by spočívala v relatívnej určitosti predmetu – blokovanie stránok s predom neurčitým okruhom jej adresátov v čase –

²⁹⁰ Důvodová zpráva k zákonu č. 186/2016 Sb., o hazardních hrách, op.cit., s.108. Dopĺňujeme, že navrhovateľ zákona si je vedomý, že takýto prístup by vyžadovalo novelizáciu príslušných právnych predpisov o zavedenie zvláštného druhu súdneho konania a predbežného opatrenia.

²⁹¹ HENDRYCH, Dušan et al. Správní právo - Obecná část. Vyd. 9. Praha: Nakladatelství C. H. Beck, 2016, 826s. ISBN 9788074006241. s.126

prevádzkovateľov nelegálnej hry na internete²⁹². Negatívne vymedzenie v SR ponecháva značný priestor k formálnemu vymedzeniu podmienok vydania a označenia opatrenia podľa ZoHH. V materiálnom poňatí, ku ktorému sa prikláňa prax súdneho prieskumu, by ZoHH stanovoval správny úkon hlavne do obsahovej stránky, ktoré by napĺňali znaky opatrenia obecnej povahy a nie jeho formy, čo vzhľadom k problematike, ktorú by upravoval nemuselo byť vhodne zvolenou úpravou. Prístup európskych prevádzkovateľov povolených hazardných hier by tak neurčitost' sémantiky a nové povinnosti mohli odradzovať od vstupu do českého sektoru. Návrh opatrenia o blokácii s odôvodnením by sa oznamoval verejnou vyhláškou s fikciou doručenia podľa §25 SR, pričom prevádzkovateľom hazardných hier vznikla nová nepriama administratívna záťaž pravidelného sledovania diaľkovým prístupom úradnú dosku MFČR²⁹³. Podľa § 173 odst. 2) proti OOP nie je prípustný žiadny opravný prostriedok. Prevádzkovateľ však môže uplatniť pripomienky k opatreniu, na ktoré správny orgán poukáže v odôvodnení. Je však pripustená možnosť preskúmania v rámci správneho súdnictva podľa § 174 odst. 2) SR a prípadná obnova konania²⁹⁴, ak by bolo zrušené záväzné stanovisko dotknutých orgánov, ktoré boli podkladom pre návrh opatrenia obecnej povahy.

V tomto prípade by zákonom taktiež musela byť zavedená všeobecná povinnosť ISP blokovať stránky nelegálnych prevádzkovateľov, o ktorých by opatrením obecnej povahy rozhodoval regulačný orgán, keďže OOP nemôže stanovovať povinnosti nad rámec zákona. V podstate by teda slúžilo ako zoznam nelegálnych IP adries, nie nepodobný *blacklistu* ktoré by boli novelizáciou pravidelne aktualizované a doplňované²⁹⁵. OOP sa nejaví ako vhodný

²⁹² KLIKOVÁ, Alena, HAVLAN, Petr a CHADIMA, Marek et al. *Správní řád*. Vyd. 2. Praha: Wolters Kluwer, 2016, 652s. ISBN 9788074789434. s.431

²⁹³ V kontexte si treba uvedomiť, že veľký prevádzkovatelia hazardných hier zvyčajne prevádzkujú hry v mnohých štátoch s rôznou právnou úpravou, je preto dôvodne možné, že by mohli ČR opomenúť expiráciu riadneho povolenia k prevádzkovaniu činnosti a stať sa súčasťou OOP o blokovaní ich stránky.

²⁹⁴ SKULOVÁ, Soňa et al. *Správní právo procesní*. Vyd. 3. Praha: Aleš Čeněk, 2017, 421s. ISBN 9788073806880. s.380

²⁹⁵ Důvodová zpráva k zákonu č. 186/2016 Sb., o hazardních hrách, op.cit., s.109

inštitút kvôli komplikovanosti problematiky, administratívnej záťaži a nemožnosťou podať riadny opravný prostriedok.

4.5.2 Rozbor ustanovení o blokácii nepovolených internetových hier

Po porozumení východísk *de lege lata* predložených v návrhu zákona a zákonodarcom zvolenej možnosti implementácie si v tomto bode priblížime metodiku ich praktického uplatňovania. Avšak, samotná existencia výkladu ťažiskových ustanovení regulácie Ústavným súdom nás podnecuje opustiť nazeranie výlučne optikou navrhovateľa zákona *e ratione legis*, a to hlavne pri absencii iného nezáväzného doktrínálneho rozboru právnou náukou. Pre akúkoľvek ďalšiu interpretáciu je nevyhnutným uviesť plné nepreložené znenie ust. §§ 82, 84 a 123 odst. 5) ku dňu účinnosti zákona o hazardných hrách:

„§ 82

Blokace nepovolených internetových her

- (1) Poskytovatelé připojení k internetu na území České republiky jsou povinni zamezit v přístupu k internetovým stránkám uvedeným na seznamu internetových stránek s nepovolenými internetovými hrami (dále jen „seznam nepovolených internetových her“).
- (2) Na seznam nepovolených internetových her se zapíše internetová stránka, na níž je provozovaná internetová hra v rozporu s § 7 odst. 2 písm. b).
- (3) Povinnost podle odstavce 1 jsou poskytovatelé připojení k internetu povinni splnit ve lhůtě 15 dní ode dne zveřejnění internetové stránky v seznamu nepovolených internetových her.

§ 84

Seznam nepovolených internetových her

- (1) Seznam nepovolených internetových her vede a o zápisu do něj rozhoduje z moci úřední ministerstvo.
- (2) Seznam nepovolených internetových her obsahuje
 - a) adresu internetové stránky, na níž je provozovaná internetová hra v rozporu s § 7 odst. 2 písm. b),
 - b) jedinečný identifikátor platebního účtu, který je využíván k provozování internetové hry v rozporu s § 7 odst. 2 písm. b),
 - c) den zápisu a výmazu údajů uvedených v písmenech a) a b).
- (3) Ministerstvo provede neprodleně výmaz internetových stránek nebo platebního účtu ze seznamu nepovolených internetových her, pominou-li důvody pro jejich zápis do tohoto seznamu.
- (4) Ministerstvo zveřejňuje na svých internetových stránkách ze seznamu nepovolených internetových her údaje podle odstavce 2 písm. a) a b).

(5) *V řízení podle odstavce 1 se účastníkovi řízení doručuje písemnost veřejnou vyhláškou a účastníkovi řízení známého pobytu nebo sídla se písemnost zašle rovněž na vědomí.*“

§123

Přestupky právníků a podnikajících fyzických osob

(5) *Poskytovatel připojení k internetu na území České republiky se dopustí přestupku tím, že neučiní ve stanovené lhůtě opatření k zamezení v přístupu k internetovým stránkám podle § 82.*

Český exemplární přístup k regulácii blokovanja je relativne priekopníckym počinom. I cez syntézu informácií, ktoré ponúka môže svojou neurčitost'ou vyvolávať stav právnej neistoty až informačnej entropie v spoločnosti. I z týchto dôvodov sa skupina 21 senátorov Senátu Parlamentu Českej republiky návrhom podaným dňa 31.8.2016 domáhala zrušenia príslušných ustanovení § 82, 84 a § 123 odst. 5 zákona o hazardných hrách u Ústavného súdu Českej republiky. Ústavný súd dospel k záveru konformity ustanovení s ústavným poriadkom a zákonom a zároveň neboli prieskumom preukázané dôvody na ich zrušenie, teda návrh senátorov ako nedôvodný meritorne zamietol²⁹⁶ podľa §70 odst. 2 zákona č.182/1993 Sb., o Ústavním soudu. Existencia výkladu Ústavného súdu ťažiskových ustanovení regulácie nás podnecuje opustiť výlučné nazeranie optikou navrhovateľa zákona *e ratione legis*, a to hlavne pri absencii iného nezáväzného doktrinálneho rozboru právnou náukou. Senátori v návrhu vnímali zvolený inštrument blokácie ako „ústavne neprípustnú cenzúru, ktorá je realizovaná bez odpovedajúcich mantinelov - svojvoľne orgánom výkonnej moci“²⁹⁷, ktorá sa vo svojej neurčitosti nedá vzťahovať pod limitáciu legitímnym zákonným opatrením a predstavuje neprípustný zásah do slobody prejavu, práva na informácie a práva podnikat'. Návrh akcentuje neurčitost' právnej úpravy pojmovou neistotou pri posúdení povinných subjektov a miery ich nutnej súčinnosti - „poskytovateľa pripojenia k internetu“,

²⁹⁶ Srov. Nález Ústavního soudu ze dne 14. února 2017 sp. zn. Pl. ÚS 28/16 ve věci návrhu na zrušení některých ustanovení zákona č. 186/2016 Sb., o hazardních hrách, vyhlášený v Sbírce Zákonů pod Předpis (Nález) č. 95/2017 Sb., částka 37 s účinností od 31.3.2017 Dostupné i online napr. z: www.psp.cz/sqw/sbirka.sqw?cz=95&r=2017 (ďalej len ako „Nález ÚS 95/2017 Sb.“)

²⁹⁷ Citácia z Nález ÚS č. 95/2017 Sb., op.cit., bod. 6. Ústavný súd zaujal stanovisko k blokácii ako „účinné (byť nikoli dokonalé) řešení“, bod 26.

„sprístupnenie a výmaz zo zoznamu“; technického cieľa úpravy blokácie - „internetové stránky“; a prístupnosti zvoleného procesného režimu.

4.5.2.1 Vymedzenie pôsobnosti a subjektov

Prvoradou prioritou je stanovenie pôsobnosti ZoHH, ktorá sa ust. § 2 vzťahuje výhradne na hazardné hry prevádzkované na území Českej republiky. Zaujímavejší je prístup zákona v určení pôsobnosti regulácie v prípade hier prevádzkovaných diaľkovým prístupom prostredníctvom internetu. Pre zásadu teritoriality je rozhodujúcim faktorom konkretizácia posúdenia zamerania či cielenia hry na osoby, ktoré majú na území ČR bydlisko²⁹⁸. Pod takýmto zameraním, by sme si mohli predstaviť napríklad možnosť českej jazykovej mutácie hazardnej hry, využitie českej národnej meny, alebo uvedenie reklamy na hazardnú hru jej prevádzkovateľom v českých periodikách.

Ďalším predpokladom porozumenia regulácie je delimitácia subjektov, ktoré priamo i nepriamo zaväzuje. Zákon v tejto súvislosti preberá výrazovú sémantiku o ktorej krátko pojednávame euro-konformným rozborom ZoHH v kapitole 4.1. Metodické pokyny odboru 34²⁹⁹ dopĺňajú subjekty o poskytovateľov internetového pripojenia bez oprávnenia podľa príslušných predpisov, čím sa zároveň dopúšťajú priestupku podľa ust. § 118 odst. 1 písm. a). Súhrnne je poskytovateľom internetového pripojenia na území Českej republiky uložená povinnosť technicky zamedziť prístupu k stránkam z rozhodnutia MFČR zapísaným na zoznam internetových stránok s hrami nepovolenými podľa zákona o hazarde (tzv. *blacklist*), a to na základe vlastných zistení alebo z podnetu tretích osôb.

4.5.2.2 Postup zápisu na blacklist

V procese zápisu na blacklist rozhoduje z moci úradnej MFČR v správnom konaní, ktorého účastníkmi sú v zmysle ust. §27 odst. 1 písm b) a odst. 2 SŘ prevádzkovateľ nepovolenej internetovej hry a skutočný držiteľ odpovedajúcej domény, ak nie sú totožnými osobami. Rozhodnutím správny orgán v tejto veci prehlasuje, že konkrétny účastník nemá

²⁹⁸ Důvodová zpráva k zákonu č. 186/2016 Sb., o hazardních hrách, op.cit., s.121

²⁹⁹ Metodické pokyny odboru 34, 2017, op.cit., s.5

práva prevádzkovania hazardných hier na internete na území ČR. Takéto rozhodnutie je záväzné pre všetkých účastníkov ako i správne orgány³⁰⁰. Zákonným opatrením uloženia a naplnenia povinnosti rozhodnúť o zápise internetových stránok na blacklist môže dochádzať k zásahu do základných ľudských práv a slobôd, preto ako odôvodňuje predkladateľ zákona³⁰¹ je rozhodované v správnom konaní pri zachovaní všetkých procesných práv jeho účastníkov. Avšak v súlade s nálezom ÚS, prevádzkovateľ nelegálnych hazardných hier svojou činnosťou ohrozuje radu ústavne chránených záujmov (zdravie, bezpečnosť a verejný poriadok, pozn.), a pretože ide o nezákonnú činnosť, neprináleží mu ochrana ústavne chránenými hodnotami slobody prejavu a vlastníctva³⁰². V súlade s princípmi správneho súdnictva sa však pri zásahu do verejných subjektívnych práv adresáta rozhodnutia zaručuje dvojinstančnosť konania³⁰³ s odkladným účinkom pri podaní riadneho opravného prostriedku³⁰⁴ a možnosť podľa §94 SŘ prieskumné konania z moci úradnej ako dozorný prostriedok. Do úvahy prichádza i podanie žaloby proti rozhodnutiu správneho orgánu podľa §65 a násl SŘS.

K zahájeniu konania dochádza dorúčením oznámenia o zahájení správneho konania z moci úradnej jeho účastníkom. Uplatňuje sa fikcia doručenia verejnou vyhláškou podľa §84 odst. 5) ZoHH. Oznámenie bežne správny orgán spája s výzvou účastníkovi správneho konania k vyjadreniu sa k podkladom rozhodnutia so stanovením primeranej lehoty. Podklady pre vydanie rozhodnutia o zápise na zoznam internetových stránok, na ktorých je prevádzkovaná nepovolená hra by podľa nášho názoru mala pozostávať aspoň z určenia

³⁰⁰ POMAHÁČ Richard. *Základy teorie veřejné správy*. Plzeň: Aleš Čeněk, 2011, 267 s. ISBN 9788073803308. s.186

³⁰¹ Důvodová zpráva k zákonu č. 186/2016 Sb., o hazardních hrách, op.cit., s.163

³⁰² Citácia z Nález ÚS č. 95/2017 Sb., op.cit., bod 29

³⁰³ Od odvolania sa dvojinstančnosť líši priebehom v rámci interna MFČR. Tým sa nulifikuje možnosť rozhodnutím v konaní o rozklade vec zrušiť a vrátiť prvoinstančnému orgánu. Konaním o rozklade je podľa § 152 odst. 6) je možné rozhodnutie zrušiť alebo zmeniť alebo rozklad zamietnuť.

³⁰⁴ SKULOVÁ, Soňa et al., 2017, op.cit., s.71 a 275. V tomto prípade pôjde o rozklad, rozhodnutie je v prvej inštancii vydané ústredným orgánom štátnej správy.

totožnosti prevádzkovateľa a vlastníka domény, zisteniu neexistencie zákonného povolenia k prevádzkovaniu hry a pôvod zamerania tejto hry na osoby s bydliskom na území ČR.

MFČR vydá rozhodnutie o zápise na zoznam nepovolených internetových hier na základe podkladov až po obdržaní vyjadrenia účastníkov alebo márnom uplynutí stanovenej lehoty k takému vyjadreniu, tak, aby bol preukázaný stav veci nad dôvodnú pochybnosť. V opačnom prípade správne konanie rozhodnutím zastaví. Obsahom rozhodnutia o zápise údajov na blacklist je identifikácia adresy internetovej stránky, na ktorej je internetová hra v rozpore s § 7 odst. 2 písm. b) prevádzkovaná. Tá pozostáva z TLD (z anglického Top Level Domain, pozn.), teda domény najvyššieho rádu (napr. národná .cz, alebo generická .org) a sub-domény ako zvoleného mena adresy prevádzkovateľa (napr. *pokerovahra.cz*, *nepovolenyhazard.org*).

V zmysle § 152 SŘ môže účastník proti rozhodnutiu podať rozklad, ktorý má suspenzívny účinok na rozhodnutie o zápise na blacklist. Devolutívny účinok mať z povahy rozhodnutia v prvej inštancii MFČR, ktoré nemá vyšší nadriadený správny orgán³⁰⁵. Tým sa bude zaoberať nezávislá päťčlenná odborná rozkladová komisia, ktorá predkladá ministrovi financií návrh rozhodnutia. Uplynutím lehoty k podaniu rozkladu, popr. oznámením (doručením), rozhodnutia ministra financií o rozklade, naberá rozhodnutie o zápise na zoznam nepovolených internetových hier právnu moc. Nepôsobí však ako počiatok 15 dňovej lehoty určenej k realizácii zákonnej povinnosti ISP. Tá začína podľa § 82 odst. 3 zákona o hazardných hrách plynúť, dňom nasledujúcim po dni zverejnenia adresy internetovej stránky v zozname nepovolených internetových hier. Z rétoriky zákonodarcu v ust. § 84 odst. 3 je zrejmé, že povinnosť ISP blokovať prístup k stránkam na blackliste trvá po celú dobu ich zápisu v zozname. V prípade pominutia dôvodov ich zápisu, MFČR vydáva nové správne rozhodnutie o ich odstránení zo zoznamu. Z dikcie zákona nevyplýva povinnosť správneho orgánu zvlášť informovať ISP o rozhodnutiach vo veciach aktualizácie blacklistu, nakoľko nie je účastníkom správneho konania. Vzhľadom k ich relatívne vysokému počtu, by to predstavovalo náročnú administratívnu úlohu, a teda k splneniu povinností pre ISP nevyhnutné odoberať RSS kanál MFČR, prostredníctvom ktorého sú

³⁰⁵ *Ibid.*, s.277

všetky rozhodnutia nových zápisov a výmazov zoznamu aktualizované. Zákon výslovne nerieši však akúkoľvek náhradu administratívnej záťaže ISP spojenou s nepretržitým sledovaním blacklistu.

Vo výsledku, ale môžeme hodnotiť takúto úpravu ako výsostne nutnú, nelegálny prevádzkovatelia hazardných hier zámerne sledovaním rôznych výhod vykonávajú službu zo zahraničia, kde by rozhodnutie o zablokovaní stránok na českom trhu bolo vymáhať takmer nemožné. Jediným dosiahnuteľným subjektom, ktorý má v technickej moci toto rozhodnutie realizovať je práve český ISP, ničmenej ako zdôrazňuje Ústavný súd, prenesením zodpovednosti za blokovanie musí ísť o takú formu rozhodnutia, ktorá podlieha riadnemu prieskumu v správnom súdnictve³⁰⁶.

Spôsob technického riešenia zamedzenia prístupu k internetovým stránkam uvedeným na blackliste sa ponecháva na úvahe ISP. Vybraný spôsob nemôže odporovať ústavne zaručeným slobodám, preto by bolo nevhodné zvolené blokovanie na úrovni dynamických IP adries, čím by neobratne mohlo dochádzať k zablokovaniu prístupu k doménam iných držiteľov. Metodické pokyny odboru 34³⁰⁷ navrhujú ako vhodné riešenie blokovanie na úrovni DNS, i keď z poznatkov v tejto práci by bol vhodnejší hybridný spôsob blokovania IP a DNS. V prípade nesplnenia povinnosti prijatím vhodných opatrení zamedzenia prístupu v 15 dňovej lehote sa ISPs dopustí správneho deliktu v zmysle § 123 odst. 5 za ktorý, môžu byť sankcionované pokutou do výšky 1 mil. Kč. Je založený na princípe objektívnej zodpovednosti s možnosťou liberácie pri preukázaní vynaloženia všetkého úsilia, ktoré možno požadovať aby k porušeniu právnej povinnosti zabránila.

Záverom nálezu, Ústavný súd posudzuje dotknuté ustanovenia ZoHH vo svetle zahraničnej, hlavne európskej úpravy³⁰⁸, v ktorom špecificky invokuje recitál 13 a čl. 3 Nariadenia (EÚ) 2015/2120 ako príklad možnej povinnosti plniť rozhodnutie verejných orgánov o blokovaní obsahu, čo kopíruje naše pochopenie nariadenia v bode 4.1.1. Ďalším

³⁰⁶ Citácia z Nález ÚS č. 95/2017 Sb., op.cit., bod 32

³⁰⁷ Metodické pokyny odboru 34, 2017, op.cit., s.10

³⁰⁸ Kritický náhľad posúdenia diplomovej práce so závermi Nálezu ÚS č. 95/2017 Sb., op.cit., bod 43 a násl.

východiskom je recitál 5 odporúčenia Komisie 2014/478/EU ³⁰⁹ , poukázaním na nedostatočný harmonizačný základ a možnosť členských štátov chrániť cieľe verejného záujmu stanovením prístupu k hazardným hrám i možnosťou obmedzenia cezhraničného poskytovania vhodnými a potrebnými opatreniami. Do úvahy treba vziať aj originálne znenie transponovanej smernice o e-obchode vo vzťahu k ISP *mere conduit*, ktoré čl. 12 odst. 3 ponecháva na možnosť súdu alebo správneho orgánu požiadať ISP o ukončenie alebo predchádzanie protiprávnej činnosti.

³⁰⁹ Odporúčenie Komisie 2014/478/EU zo 14. júla 2014 o zásadách ochrany spotrebiteľov a hráčov využívajúcich služby online hazardných hier a o predchádzaní hraniu online hazardných hier v prípade maloletých osôb. Dostupné i online z: publications.europa.eu/sk/publication-detail/-/publication/f84fa393-0f01-11e4a7d0-01aa75ed71a1/language-sk

Záver

Úlohou tejto práce bolo analyzovať históriu a vývoj dvoch veličín internetu a regulácie v priebehu času, a skúmať jeho súčasné východiská pre subjekty nadané *umením riadenia*. Pomocou analógií a metafor sa snažíme pochopiť:

- a) ako sa táto technológia a tradičná regulácia vzájomne ovplyvnili a vyvinuli do bodu, v ktorom sú dnes,
- b) dôvod na prispôbenie regulácie, ktorá by vyhovovala potrebám internetu vo forme, v akej existuje dnes, a
- c) navrhnúť riešenie: ako môže byť internet vhodne regulovaný v budúcnosti.

Ak by sme sa vrátili späť v čase a viedli odborný rozhovor s tvorcami internetu, je bez akejkoľvek pochybnosti, že ich reakcia na to, ako sa internet vyvinul, by zaviedol odbornosť rozhovoru do nadšeného smiechu, prekvapenia, či nemého úžasu. Môžeme tvrdiť, že toto experimentálne úsilie pôvodných tvorcov nebolo vedené s cieľom vyvinúť internetovú sieť do behemota, akým je dnes. Skutočnosť je taká, že vznik a rast internetu nebol plánovaný a dobre premyslený a jeho postup nebol riadený, dokonca ani financovaný jediným orgánom. To, čo sa začalo ako sieť spájajúca jeden počítač s druhým, sa vyvinulo do organickej globálnej spoločnosti s vlastnou infraštruktúrou, pravidlami a reguláciou, pričom mnohí jej aktéri používajú rovnakú technológiu na podporu rozdielnej izolovanej agendy. Tak ako sa dynamicky vyvíjala internetová infraštruktúra, jej podstata a služby, tak nezaostávalo ani chápanie jej regulácie. Rôzne definičné authority si utvárali vlastné predstavy a k tomu organicky aplikovali vlastné pravidlá a kódy, ktorými sa časť kybernetického priestoru riadila a regulovala. Od počiatku však chýbala ucelenosť či aspoň názorová unifikovanosť. V podstate sa odohrával skrytý boj o moc nad objektom medzi spoločnosťou a štátom. Internet vo svojej nehmotnej podobe je dodnes spleťou sieťou o ktorej sa zdá, že nadobudla svoj vlastný tvar bez celistvého rámca koľajníc na usmerňovanie svojho rastu smerom k vopred nevyznačenému cieľu.

Diplomová práca pozostávala takmer výlučne z právne technického výkladu abstraktných pojmov a ich reálnej aplikácie. V závere by preto k účelom pochopenia tohto javu bolo osviežujúcim použiť hravú analógiu pripodobnenia nehmotného k dobre známemu.

Predstavme si civilizáciu, ktorá si neuvedomuje možnosti sveta, ktorý existuje mimo ich mestských hradieb. Avšak malá skupina zvedavých prieskumníkov cestuje za mestské hradby, prechádza cez hory a rieky aby sa dostala do ďalšieho mesta, kde sa stretne s inou civilizáciou. Prieskumníci nadväzujú cenné kontakty a rozhodnú sa začať spoločnú iniciatívu budovania ciest a mostov [*sietové prepojenie medzi počítačmi*] medzi spriatel'enými mestami. Cesty sú postavené bez iného zámeru či účelu, ako len spojiť tieto dve mestá. Myšlienka ktorá uľahčuje cestovanie, je nová, ale nepriťahuje veľkú pozornosť vodcov ktorejkoľvek civilizácie, nazdávajú sa, že ide o experiment medzi niektorými občanmi s potenciálom, ktorý si snáď ani dobre neuvedomujú. Cesty fungujú dobre a nie sú využívané už len zvedavcami z oboch miest, ale ako myšlienka začína získavať trakciu vytvárajú sa spoločenské siete medzi viacerými mestami [*prijatie internetu medzi viacerými používateľmi, vytvorenie väčšej siete*].

Rozvoj týchto ciest sa uskutočňuje na základe vzájomnej dôvery medzi zúčastnenými občanmi. Cesty získavajú popularitu, začína ich využívať čoraz viac ľudí a ich účel sa mení, voľba jeho smerovania však zostáva občanovi. Spočiatku je využívaná hlavne k rýchlej výmene správ – komunikácie medzi mestami [*základný e-mail*]. Ako sa vyvíja technológia, tak sa vyvíja i infraštruktúra týchto ciest [*nový TCP/IP protokol*], aj spôsob dopravy od vynálezu koňských záprahov k automobilom [*Pripojenie z osobných počítačov sa vyvinuli na pripojenie z prenosného počítaču*]. Rôzne účely, pre ktoré tieto cesty slúžia, sa začínajú vyvíjať rovnakým tempom. Niektorí občania si popri ceste dokonca otvorili malé stánky s tovarom spohodľujúcim cestu občanom [*programové aplikácie a služby WWW*]. Koncept hmotných ciest / sietí sa vyvinul na nehmotné cestovanie vo vzdušnom priestore [*kábel do wifi*]. Rýchlosť, ktorou sa občania presúvali, exponenciálne stúpala [*od dial-up až po pripojenie 5G*].

Účel týchto sietí sa rozvinul tak, aby zahŕňal nielen zdieľanie informácií, ale i obchod a zábavu [*celosvetový internet, online nakupovanie, sociálne médiá, streamovanie televízie a hranie hier*] a predtým, ako si to sami stihli uvedomiť vznikla nová forma spoločnosti

[kyberpriestor]. Občania / používatelia [*poskytovatelia obsahu, poskytovatelia internetových služieb, koncoví užívatelia*] "ciest" s cieľom vyhnúť sa hrozbe absolútnej regulácii štátu a vlády sa rozhodli samoregulovať, ale trpká skutočnosť nastala v uvedomení, že rovnako ako cesty sú využívané pre hodnotnú, tvorivú a obchodnú činnosť, ktorá bola životne dôležitá pre ich vývoj - pritiahla aj pirátov, zlodějov, vrahov a násilníkov [*hackeri, pornografické webové stránky, krádeže identity, nezákonné hranie hazardných hier*]. Rovnaké cesty, ktoré uľahčujú vynaliezavosť a pokrok, sú totiž tie isté cesty, ktoré zločincovi zjednodušujú páchanie svojich zločinov, ktorí tak majú dosah na oveľa väčší počet obetí, než kedykoľvek predtým. Občania sa pokúšali vytvoriť brány a postavili strážu pozdĺž ciest, ale chýbali im k tomu nástroje vymáhania a náznaky konzistentnej aplikácie. Skutočnosťou bolo, že žiadny používateľ nebol považovaný za zodpovedného za ochranu a riadenie týchto ciest. Totiž keď sú zodpovední všetci, zodpovedný nie je nikto. Samozrejme, lídri každej civilizácie začali riešiť problémy *ad hoc*, pretože napriek počiatkovej implicitnej vzájomnej dôvere medzi občanmi nemožno ju dlhodobo považovať za samozrejmosť. Tak ako všetci začali tieto siete využívať a našli v nich vlastné hodnoty, tak isto učinili i devianti v spoločnosti. Vedúci predstavitelia každej príslušnej spoločnosti si nikdy nedokázali predstaviť, že to, čo sa začalo ako obyčajné experimentovanie medzi malým počtom občanov, by sa vyvinulo do takej miery. Lídri, ktorí kedysi umožnili a podporili samoreguláciu týchto sietí, začali vidieť potrebu regulácie, aby sa zabezpečilo, že ich občania budú chránení a že zákony, ktorými riadili svoju krajinu budú v rovnakej miere implementované aj na týchto cestách / sieťach.

Keď sa všetci prebudili z opojného sna samoregulovaného kyberpriestoru ciest čelili nasledujúcim problémom:

1. Komu vlastne skutočne patria tieto cestné infraštruktúry?
2. Cesty siete teraz pokrývajú územie celého sveta, ale koho vládou sa riadia?
3. Občania, ktorí si zvykli na samoreguláciu týchto sietí, začali protestovať proti myšlienke, že títo lídri náhle vstúpia a pokúsia sa regulovať svoje "slobodné" siete.
4. Ako by však mohli byť občania chránení pred zločincami, ak by sa právne predpisy miest neuplatňovali konzistentne i na tieto siete ciest?

5. Ak by sa zákony mali presadzovať, kto by bol skutočne zodpovedný za presadzovanie zákonov?

Aby sme zmysluplne odpovedali na niektoré z týchto otázok a nezamotali sa do chaosu, vráťme sa späť k tomu, ako sa tieto cesty vytvorili medzi mestami. Každé mesto malo vlastnú formu riadiaceho rámca [*vlády*]. Koncepcia modernej spoločnosti existovala od doby ako si občania uvedomili, že je v ich najlepšom záujme, aby boli vedený vodcami, ktorých si zvolili, komu by odovzdali určité prirodzené slobody. Odmenou im bolo vytvorenie poriadku, v ktorom pravidlá a predpisy budú vládnuť občanom. Iba tak mohli byť ochránené spoločné záujmy spoločnosti a zabezpečiť vlastné prežitie. Vytvorili s vodcami spoločenskú zmluvu. Z tejto analógie je zrejmé, že vzhľadom na skutočnosť, že občania reálneho sveta sa rozhodli existovať ako súčasť spoločnosti a byť riadení demokratickými vládami, je logické, že tá istá logika by sa mala vzťahovať na internet. Čo iného je internet ak nie iba spoločnosť v rámci spoločnosti?

Skutočnosť spočíva v tom, že žijeme v spoločnosti riadenej pravidlami a nariadeniami. Internet ako jej integrálna súčasť existuje taktiež, len v priestore povolenom vládou. Len preto, že sa vyvinula z niečoho malého do mýtického behemota, a fakt, že teraz sa snažíme tento vývoj dosiahnuť v akejsi hre na *riadenie*, neznamená, že by vláda stratila svoju legitimitu, motív či prostriedky. Jediné čo stratila na cestách je efektivita tohto riadenia.

Avšak, ak sme sa ako ľudia rozhodli byť *riadení* v reálnom svete a byť súčasťou spoločnosti pre vzájomný prospech členov tejto spoločnosti, prečo zrazu chceme mať ilúziu slobody v novom priestore? Táto sloboda je iba utopickou ilúziou, pretože aj keď to nie sú výlučne vlády, ktoré regulujú alebo riadia túto platformu, skutočnosťou je, že je často regulovaná iným netransparentným spôsobom. Zvyčajne odovzdávame moc autoritatívnym inštitúciám štátu výmenou za ochranu našich slobôd a táto zvolená demokratická sila potom určuje pravidlá a predpisy našej spoločnosti. Tieto predpisy sú transparentné a ľudu je priznané hlavné *slovo* v tom kto a akú reguláciu tvorí. Takéto súkromné subjekty, ktoré kódom samoregulujú internetovú realitu však konajú presne opačne. Algoritmy, optimalizácia internetových vyhľadávačov, správa siete, blokovanie a filtrovanie, zneužívanie osobných údajov. Tým vymenúvame len niekoľko z mála problémov, ktoré nie

sú dostatočne ošetrované. Užívatelia o nich často nevedia, a aj keď nemajú veľké slovo pri ich zavádzaní sú nimi nepriamo postihovaní či zaväzovaní.

Je namieste pochopiť, že záujmom týchto subjektov je tvorba finančného kapitálu, a nie ochrana našich práv a zlepšenie spoločnosti ako celku. Akákoľvek argumentácia proti regulácii internetu je v skutočnosti neúplná, internet je regulovaný vždy - či už súkromnými subjektmi, morálnym kódexom alebo vládou. To, ako sme zdôraznili, čoho by sa mali občania kybernetického priestoru skutočne obávať, je nový regulátor - architektúra kódu. Vo svojej podstate je nestály, používa sa nekonzistentne a subjektívne a chýba mu transparentnosť, ktorú zákonné normy naopak poskytujú. Kód existuje tiež s mnohými skrytými vrstvami, ktoré nie sú zjavné pre používateľov, a môžu byť zmenené rýchlo a bez vedomia alebo dokonca súhlasu používateľov. Zákon demokratického štátu takto v porovnaní poskytuje aspoň vytúženú právnu istotu.

Prostredníctvom štúdia rôznych prípadov, zákonov, článkov a rámcových regulácií, sa táto práca vydala na cestu pochopenia povahy internetu a jeho regulácie v priebehu času. Vybavení týmito znalosťami a porozumením sa snažíme navrhnúť optimálny regulačný rámec pre internet a pomocou metafor a analógií vysvetliť jeho spôsobilosť súčasnému a budúcemu občanovi kybernetického priestoru.

Diskusia o súkromnej a verejnej regulácii alebo silnej štátnej regulácii a deregulatívnym formám prebieha roky bez jasného víťaza. Ako sme poukázali, nie je v našom najlepšom záujme obísť štátne nariadenia, ktoré chránia záujmy spoločnosti. Nemôžeme sa však vzdať toho, že samoregulácia internetu efektívne umožnila rýchly rast a vývoj a podporila inovácie a podnikanie. Taktiež, vzhľadom na veľkosť internetu a rýchlosť rozširovania informácií by bolo ťažké, ak nie nemožné, aby samotný štát efektívne spravoval taký rozsiahly priestor. Na rozdiel od toho, že argumentujeme pre a proti ktorémukoľvek z týchto modelov regulácie, rozhodli sme sa podporiť oboje zdôraznením rámca, ktorý dokáže vytvoriť hybrid oboch metód regulácie a realisticky zabezpečiť, aby regulácia internetu bola viac štruktúrovaná a konzistentná. Na reguláciu internetu je navrhovaný rámec metaregulácie, ktorá poukazuje na štátny dohľad v kontexte monitorovania implementácie opatrení súkromným subjektom. Už napríklad Ayres a Braithwaite postulovali modernú

rozsiahljšiu koncepciu metaregulácie, ktorá víta rozmanitosť prístupov štátnych a neštátnych inštitúcií. Vo svojej práci položili základ novej metaregulačnej teórie, pričom konštatujú, že nariadenie môže byť delegované a takéto delegovanie môže byť monitorované štátom³¹⁰.

Keďže sa veľa inšancií samoregulácie internetu vytvorilo historicky ako *spontánny poriadok*, táto regulačná štruktúra zabezpečí, že prostredníctvom zavedenia metaregulácie štátom sa táto odroda samoregulácie s nadväznosťou na Hayeka bude pohybovať v rámci úmyselne vytvoreného poriadku, teda tých istých zákonov, aké uplatňuje štát v reálnom svete. Dodržiavanie tohto rámca vznikne organicky, i keď pod legitímnou hrozbou uplatnenia sankcie nastavenej štátom. Delegovanie určitých regulačných úloh na ISP je pre štáty rovnako príťažlivým návrhom, pretože nemajú dostatočný technický prístup a prostriedky dohliadania a vynucovania určitých noriem. Ako príklad vhodne poslúži zavedenie blokovania nelicencovaných hazardných stránok v ZoHH. Prostredníctvom tohto delegovania aplikácie regulačného rámca, ISP preberajú dvojakú úlohu ako správcovia a tvorcovia definičných noriem bez toho, aby sa od štátu vyžadovala enormná investícia do nového dohľadného orgánu pre presadzovanie práva na internete.

Na to, aby štát vypracoval efektívny rámec metaregulácie internetu, je dôležité, aby:

1. štát rozumel novej technológii. K odvodeniu rámca metaregulácie by bolo vhodné prijať poradenstvo technického konzultanta, aby sa zabezpečilo zohľadnenie všetkých úrovní internetového kódu / infraštruktúry;
2. bol dodržiavaný kód a zodpovednosť, ktorá je delegovaná na poskytovateľov, je praktická a zároveň neporušuje, ale chráni práva koncových užívateľov. Príkladom by bolo vyžadovanie proaktívnej blokácie obsahu, v prípade ktorý porušuje základné ľudské práva od poskytovateľov služieb informačnej spoločnosti. Táto

³¹⁰ DRAHOS, 2017, op.cit., s.150. Je poukázané na prácu AYRES, Ian a BRAITHWAITE, John. *Responsive Regulation: Transcending the Deregulation Debate*. New York: Oxford University Press, 1992. Dostupné z: johnbraithwaite.com/wp-content/uploads/2016/06/Responsive-Regulation-Transce.pdf

žiadosť by znamenala vytvorenie mechanizmov na skenovanie a analýzu obsahu, ktorý prechádza ich sieťami. Nevhodne zvolený kód mechanizmu, by mohol narušiť súkromie koncových užívateľov a slobodu prejavu rovnako ako nechť vstupu nových súkromných subjektov do odvetvia.

Vyššie uvedený bod vyvoláva diskusiu, o ktorej hovoril Lessig. Mal by štát regulovať kód? V tomto okamihu je to fixný kód, ktorý je prekursorom architektúry internetu, pričom regulácia sa často prispôsobuje pre-existentnému kódu. Tento scenár by sa však mohol obrátiť, ak zákon stanoví kódex internetu, ktorý by vyhovoval jeho regulačnému rámcu. Opäť najlepšie riešenie nie je vyberať izolovane jedno alebo druhé, ale vytvoriť symbiotické prostredie medzi kódom a zákonom a ostatnými *definičnými normami*, ktoré sa vzájomne prispôbujú.

Vráťme sa k použitiu analógie *cesty / siete* v reálnom svete, aby sme opísali toto metaregulované riešenie internetu. Predstavme si, že demokratické štáty sú navzájom prepojené diaľnicami [*infraštruktúry internetových sietí*]. Cesty sú postavené stavebnými inžiniermi [*technológmi*], ktorí majú know-how a odborné znalosti o tom, ako rozložiť cestné siete a infraštruktúru mesta, ale plánovanie infraštruktúry [*tradičná regulácia*] vykonáva štát, aby sa zabezpečilo, že slobodné a spravodlivé demokratické prostredie bude odzrkadlené v mestskej a cestnej architektúre. Sú voľne prístupné pre všetkých, za predpokladu získania vodičského preukazu [*zmluva s poskytovateľmi pripojenia k internetu*]. Štáty regulujú cesty vytvorením rámca pravidiel, ktoré musí dodržiavať každý vodič [*užívateľia / poskytovatelia obsahu*] a licenčné oddelenie [*ISP*]. Každé licenčné oddelenie vytvára vlastné predpisy, ale zostáva v rámci vytvoreného štátom. Ak sa nedodržia tieto metaregulačné rámce, môžu podliehať sankciám alebo ich možnosť udeľovať licencie by mohla byť úplne pozastavená alebo zrušená. V niektorých prípadoch štát vytvára podnety pre proaktívne opatrenia prijaté oddeleniami na udeľovanie licencií na dodržiavanie ľudských práv, ako je napríklad pomoc pri hľadaní neoprávnených vodičov, ktorí spôsobili nehody na ceste (po podaní sťažnosti / policajnej správy) [*blokovanie / odstránenie určitého obsahu alebo webových stránok považovaných za nezákonné*].

Všetci oprávnení vodiči majú garantovaný rovnaký prístup ku všetkým cestám [*net neutrality*]; bez ohľadu na to, či ide o jediného vodiča [*koncového používateľa*], malé rodinné

vozidlo [*blogovú webovú stránku*], obchodný kamión [*služby Amazon / eBay*], ktorý prepravuje tovar, alebo verejný autobus [*sociálne siete médií*]. Cesty sa riadia dopravnými zákonmi, ktoré sú súčasťou zákonného rámca, ale realizáciu týchto zákonov vykonáva dopravné oddelenie [*správne orgány*] v spolupráci s licenčným oddelením [*ISP*]. Obmedzenia rýchlosti stanovuje dopravné oddelenie [*rýchlosti liniek zakúpených prostredníctvom poskytovateľov internetových služieb*]. Dopravné oddelenie dovoľuje riadenie premávky súkromným subjektom [*prevádzka siete ISP*], ale kladie si podmienky na jeho výkon tak, aby sa nevyskytoval žiaden nespravodlivý favoritizmus a so všetkými európskymi vodičmi bolo zaobchádzané rovnako a spravodlivo.

K základným trom otázkam z úvodu práce sa musíme postaviť nasledovne. Tradičná regulácia je výslovne nutná do miery, v ktorej je vytváraná efektívne v symbióze s kódom novej technológie a *vice versa*. Prostredie internetu sa tak organicky oslobodí z pút nevhodnej rigidity, ale zároveň budú zaručené nielen práva občanov totožne ako v reálnom svete ako i nastavený morálny štandard spoločnosti. Preto odpoveďou nie je jednoducho – *metaregulácia*, ale taktiež unifikovaný hlas legislatívnej tvorby a subjektov regulácie na Lessigovské „regulovať správne či dobre?“ musí znieť - *oboje*. Iba takáto *informácia* je totiž schopná skutočného zvýšenia miery organizácie spoločnosti ako celku.

Zoznam použitých zdrojov

1. Zoznam použitej literatúry

- ADAME, Talia. *Handbook of Cybernetics*. rev. Vyd. 2016. New York: Library Press, 2016
- ANDRUŠKO, Alena. *Internet, informační společnost a autorské právo*. Praha: Wolters Kluwer ČR, 2016
- BALDWIN, Robert, CAVE, Martin a LODGE, Martin ed. *The Oxford handbook of regulation*. Vyd. 1. Oxford: Oxford University Press, 2010
- BARTÁK, Matěj, VEBROVÁ, Jitka a RYCHLÁ, Renata ed. *Nový slovník cizích slov pro 21. století*. Praha: Plot, 2008
- BARZILAI-NAHON, Karine. Gatekeeping: A critical review. *Annual review of Information Science and Technology*. 2009, roč. 43, č.1, s.433-478. ISSN 0066-4200. s.433
- BAWDEN, David a ROBINSON, Lyn. The dark side of information: overload, anxiety and other paradoxes and pathologies. *Journal of Information Science*. 2009, roč. 35, č.2, s.180-191
- BAYEROVÁ, Monika. Evropská úmluva o počítačové kriminalitě a sexuální zneužívání dětí. *Trestněprávní revue*, Praha: C.H.Beck, 2003, roč. 2, č. 5, s. 156-157
- BELLIA, Patricia L., BERMAN, Paul Schiff a POST, David G. *Cyberlaw: problems of policy and jurisprudence in the information age*. St. Paul, MN: Thomson/West, 2003
- BONY, Elizabeth de. European Union Sees Need to Regulate 'Net'. *ComputerWorld*. 1996, roč. 30, č. 43, s.90
- BOYLE, J. *Shamans, Software, and Spleens: Law and the Construction of the Information Society*. Cambridge, MA: Harvard University Press, 1997
- BREIDENBACH, Susan. Future of High Speed Networks. *NetworkWorld*. 2000, roč. 17, č. 7, s. 67-68
- COGLIANESE, Cary. a KAGAN, Robert A. *Regulation and regulatory processes*. Burlington, VT: Ashgate, 2007
- DOUZINAS, Costas a GEAREY, Adam. *Critical jurisprudence: the political philosophy of justice*. Oxford, UK: Hart Publishing, 2005
- DRAHOS, Peter ed. *Regulatory theory : foundations and application*. Acton, AU: ANU Press, 2017
- DRUCKER, Peter F. *The Age of Discontinuity*. Oxford, UK: Butterworth-Heinemann, 1969
- EASTERBROOK, Frank H. *Cyberspace and the Law of the Horse*. University of Chicago Legal Forum, Roč. 1996, s.207-216
- EDWARDS, Lilian. a WAELDE, Charlotte. *Law and the Internet*. 3rd ed. Portland, OR: Hart Publishing, 2009
- FEELEY, Matthew J. EU Internet Regulation Policy: The Rise of Self-Regulation. *Boston College International and Comparative Law Review*. 1999, Roč. 22, č. 1, s. 159 – 174
- GERLOCH, Aleš. *Teorie práva*. 3. rozš. vyd. Plzeň: Aleš Čeněk. Právnické učebnice (Aleš Čeněk), 2004

GIBBONS Llewelyn Joseph. No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace. *Cornell Journal of Law and Public Policy*. 1991, Roč. 6, č.3, s. 475-551

GIBSON, William. *Neuromancer*. New York: Ace Books, 1984.

GRAHAM J. H. SMITH. *Internet Law and Regulation*. 4. ed. London: Sweet & Maxwell, 2007

GRÍVNA, Tomáš, POLČÁK, Radim et al. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008

GUNNINGHAM, Neil, REES, Joseph. Industry Self-Regulation: An Institutional Perspective. *Law&Policy*. 1997, Roč. 19, č. 4, s. 363-414

HARAŠTA, Jakub. Obecná prevenční povinnost poskytovatele služeb informační společnosti ve vztahu k informacím ukládaným uživatelem. *Právní rozhledy*, Nakladatelství C.H. Beck. 2014, roč. 2014, č. 17, s. 590-593

HAYEK, Friedrich August von. *Právo, zákonodárství a svoboda: nový výklad liberálních principů spravedlnosti a politické ekonomie*. Přeložil JEŽEK, Tomáš. Praha: Prostor, 2011

HENDRYCH, Dušan et al. *Správní právo - Obecná část*. Vyd. 9. Praha: Nakladatelství C. H. Beck, 2016

HUSOVEC, Martin. *Zodpovednosť na internete: podľa českého a slovenského práva*. Praha: CZ.NIC, 2014

INSTITUTE, Government. *Telecommunications: Glossary of Telecommunications Terms*. Rockville, MD: Government Institute, 1998

JAFFE Adam B.; LERNER Josh; STERN Scott. *Innovation policy and the economy*. Cambridge, MA: National Bureau of Economic Research, 2001

JANSA, Lukáš, PETR OTEVŘEL, Jiří ČERMÁK, PETR MALIŠ, PETR HOSTAŠ, MICHAL MATĚJKA a JÁN MATEJKA. *Internetové právo*. Brno: Computer Press, 2016

JELÍNEK J. et al. *Trestní právo procesní*. 4. vyd. Praha: Leges, 2016

JELÍNEK J. et al. *Trestní zákon a trestní řád s poznámkami a judikaturou*. 7. vyd. Praha: Leges, 2017

JOHNSON, D.R. a POST D.G. Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*. 1996, Roč. 48, č. 5, s. 1366-1402

KLIKOVÁ, Alena, HAVLAN, Petr a CHADIMA, Marek et al. *Správní řád*. Vyd. 2. Praha: Wolters Kluwer, 2016

KNAPP, Viktor. *Teorie práva*. Vyd. 1., 3. dot. Praha: C.H. Beck. Beckovy právnické učebnice, 1995

KOSEK, Jan, WEINBERGER, Ota a KUBEŠ, Vladimír, ed. *Brněnská škola právní teorie: (normativní teorie)*. Praha: Karolinum, 2003

LAIDLAW, Emily B. *Regulating speech in cyberspace: gatekeepers, human rights and corporate responsibility*. Cambridge, UK: Cambridge University Press, 2015

LESSIG, Lawrence. *Code: Version 2.0*. New York: Basic Books, 2006

LESSIG, Lawrence. *Free Culture: How Big Media uses Technology and the Law to Lock Down Culture and Control Creativity*. New York: The Penguin Press, 2004

- LESSIG, Lawrence. *The Law of the Horse: What Cyberlaw Might Teach*. Harvard Law Review. 1999, roč. 113, č. 3, s. 501-549
- LOFGREN, Eric T. a FEFFERMAN, Nina H.. The untapped potential of virtual game worlds to shed light on real world epidemics. *The Lancet*. 2007, roč. 7, č. 9, s. 625 - 629
- LUCA, Dumitru, SIRGHI Lucel, COSTIN Claudiu. *Recent Advances in Technology Research and Education*. Springer International Publishing, 2018
- MAISNER, Martin. *Zákon o některých službách informační společnosti: Komentář*. V Praze: C.H. Beck. Beckovy komentáře, 2016
- MATEJKA, Jan. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Vyd. 1. Praha: CZ.NIC, 2013
- NASBITT, John. *Megatrends: Ten New Directions Transforming Our Lives*. Vyd. 1. New York: Warner Books, 1982
- NORMAN, Jeremy M. *From Gutenberg to the Internet: a sourcebook on the history of information technology*. Novato, CA: Historyofscience.com, 2005
- PIOTROWSKY, Robert. Between Plato and Wiener. Philosophical cybernetics in the 17th century. *Studies in Logic, Grammar and Rhetoric*. Roč. 2012, č. 28(41), s.63-71
- POLČÁK, Radim, ŠKOP, Martin a MACEK, Jakub. *Normativní systémy v kyberprostoru: (úvod do studia)*. Brno: Masarykova univerzita, 2005
- POLČÁK, Radim. *Informační teorie práva*. In Komunistické právo v Československu. 1. vyd. Brno: Masarykova Univerzita. s. 167-176. Mezinárodní politologický ústav, 2009
- POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, edice Téma, 2012
- POLČÁK, Radim. Odpovědnost poskytovatelů služeb informační společnosti (ISP). *Právní rozhledy*, Praha: C.H.Beck. 2009, roč. 2009, č. 23, s. 837-841
- POLČÁK, Radim. *Právo na internetu: spam a odpovědnost ISP*. Brno: Computer Press. Právo a IT, 2007
- POMAHÁČ Richard et al. *Veřejná správa*. Vyd. 1. Praha: C.H.Beck, 2013
- POMAHÁČ Richard. *Základy teorie veřejné správy*. Plzeň: Aleš Čeněk, 2011
- POSNER, Richard A. Response, Legal Pragmatism Defended. *University of Chicago Law Review*. Roč. 2004, č. 71.2, s. 683-690
- POUPEROVÁ, Olga. *Institucionální aspekty regulace médií*. Vyd. 1. Praha: Wolters Kluwer ČR, 2016
- PRŮCHA, Petr. K pojetí správněprávní odpovědnosti a správního trestání. *Správní právo*. Praha: Ministerstvo vnitra. 2014, roč. 2014, č.1-2, s. 16-27
- REIDENBERG, Joel R. Governing Networks and Rule-Making in Cyberspace. *Emory Law Journal*. 1996, roč.45, s. 911-930. ISSN 0094-4076
- REIDENBERG, Joel R. States and Internet Enforcement. *University of Ottawa Law & Technology Journal*. 2003, roč. 1, č. 1-2, s. 213-230

- SHOEMAKER, Pamela J. a VOS, Tim P. *Gatekeeping theory*. New York: Routledge, 2009
- SCHRÖDINGER, Erwin. *What is life?: the physical aspect of the living cell*. New York: Cambridge University Press, 1992
- SKULOVÁ, Soňa et al. *Správní právo procesní*. Vyd. 3. Praha: Aleš Čeněk, 2017
- SMEJKAL, Vladimír, a kolektiv. *Právo informačních a telekomunikačních systémů*. 2. aktualizované a rozšířené vydání. Praha: C.H.Beck, 2004
- SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň : Aleš Čeněk, 2015
- SMEJKAL, Vladimír. Počítačová a internetová kriminalita v České republice. *Právní rozhledy*. 1999, roč. 1999, č. 12, s. 1 - 24
- SMEJKAL, Vladimír. *Internet a §§§*. Praha: Grada, 2001
- SMITH, Adam. *Pojednání o podstatě a původu bohatství národů*. Přeložil Vladimír IRGL, Alena JINDROVÁ, Josef PYTELKA a Sergej TRYML. Praha: Liberální institut, 2016
- STRATE, Lance. The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication*. 1999, Roč. 63, č.3, s.382-413
- VANÍČEK Z., MATES P., NIELSEN T. *Zákon o elektronických komunikacích. Komentář*. Praha: Linde Praha a.s., 2014
- VANÍČEK, Zdeněk, MATES, Pavel a NIELSEN, Tomáš. *Zákon o elektronických komunikacích. Komentář*. Praha : Linde Praha a.s., 2014
- WEBSTER, Frank. *Theories of the Information Society*. 3. vyd. New York: Routledge, 2006
- WEISER, Philip J. Internet Governance, Standard Setting, and Self-Regulation. *Northern Kentucky Law Review*. 2001, Roč. 28, č. 4, s. 822-846
- WIENER, Norbert. *Cybernetics, Second Edition: or the Control and Communication in the Animal and the Machine*, vyd. 2. The MIT Press, 1965
- WIENER, Norbert. *The human use of human beings: cybernetics and society. With a new Introduction by Steve J. Heims*. London: Free Association, 1989
- WINKLER Petr et al. *Problémové hráčství Společenské náklady na hazardní hraní v České republice*. 1.vyd. Národní ústav duševního zdraví, 2015
- WITZLEB Norman et al. *Emerging challenges in privacy law: comparative perspectives*. Cambridge, UK: Cambridge University Press, 2014

2. Zoznam použitých digitálnych publikácií

- BARLOW, John Perry. *A Declaration of the Independence of Cyberspace* [online]. EFF, publikované 8.2.1996 [cit. 7.4.2018]. Plné nepreložené znenie dostupné z: www.eff.org/cyberspace-independence

BARZILAI-NAHON, Karine. *Toward a Theory of Network Gatekeeping: A Framework for exploring information control* [online]. Network Gatekeeper, publikované 12/2007 [cit. 10.4.2018]. Dostupné z: ekarine.org/wp-admin/pub/GatekeepingSalienceTheory.pdf

CZ.NIC *Společná deklarace o spolupráci v rámci provozu linky pro hlášení nezákonného obsahu* [online]. [cit. 18.3.2018]. Dostupné z: https://www.nic.cz/files/nic/doc/NCOZ-20170215-deklarace_Internet-Hotline.pdf

ČTÚ. *Vyjádření Českého telekomunikačního úřadu k vybraným otázkám přístupu k otevřenému internetu a evropským pravidlům síťové neutrality* [online]. Publikované 23.3.2017 [cit. 18.3.2018]. Dostupné z: www.ctu.cz/vyjadreni-ceskeho-telekomunikacniho-uradu-k-vybrany-m-otazkam-pristupu-k-otevrenemu-internetu

DENNING, P.; HEARN, A.; KERN, C.W. *History and Overview of CSNET* [online]. Publikované 12/1982. [cit. 7.11.2017]. Dostupné: pdfs.semanticscholar.org/adae/a5be633869d79dfd6f6f23f5aa09cee92860.pdf

DG Connect. *Connected Continent legislative package*. EC.europa.eu, publikované 12.9.2013 [cit. 25.3.2018]. Dostupné z: ec.europa.eu/digital-single-market/en/connected-continent-legislative-package

Európska Komisia. *Cybercrime* [online]. [cit. 16.3.2018]. Dostupné z: ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

Európsky Parlament. *EP v boji proti sexuálnému zneužívaniu detí* [online]. Publikované 30.9.2010 [cit. 17.3.2018]. Dostupné z: europarl.europa.eu/news/cs/headlines/society/20100927STO83658/ep-v-boji-proti-sexualnimu-zneuživani-deti

FCC. *FCC Adopts Policy Statement. New principles preserve and promote the Open and Interconnected Nature of Public Internet* [online]. Publikované 5.8.2005 [cit. 25.3.2018]. Dostupné z: apps.fcc.gov/edocs_public/attachmatch/DOC-260435A1.pdf

HOLLAAR Lee A., *Legal Protection of digital information* [online]. Publikované 2002 [cit. 25.3.2018]. Dostupné z: digital-law-online.info/lpdi1.0/treatise33.html

CHLAD, Radim. *Historie Internetu v České republice* [online], Masarykova Univerzita, publikované 2000 [cit. 11.12.2017]. Dostupné z: www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm

Internet Society. *Perspectives n Internet Content Blocking: an Overview* [online]. Publikované 3/2017 [cit. 17.3.2018]. s. 5-7

JAMES, William. *Pragmatism. A new name for some old ways of thinking*. Lecture II. – What Pragmatism means? [online]. Project Gutenberg, [cit. 29.3.2018]. Dostupné z: www.gutenberg.org/files/5116/5116-h/5116-h.htm#link2H_4_0004

JOHNSON, Barnabas D. *Cybernetics of Society. The Governance of Self and Civilization* [online]. Jurlandia.org [cit 31.3.2018] Dostupné z: www.jurlandia.org/cybsoc.htm#Conclusion

KIM, Tae. *"Free Speech" in Cyberspace* [online]. 1998, [cit 7.4.2018]. Dostupné z: cyber.harvard.edu/fallsem98/final_papers/Kim.html

LA RUE Frank. *Správa osobitného spravodajcu o podpore a ochrane práva na slobodu názoru a prejavu (dokument A/HRC/17/27) zo 16. mája 2011* [online]. Rada OSN pre ľudské práva, publikované 16.5.2011 [cit. 28.3.2018]. Dostupné z: daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/17/27&Lang=E

- LANDWEBER, Lawrence. *The Computer Science Network. Asian Internet History Project* [online]. CSNET, publikované: 7.6.2012 [cit. 7.11.2017] Dostupné z: sites.google.com/site/internethistoryasia/book1/3-2-csnet
- LEE, Tim Berners. *The World Wide Web: Past, Present, Future* [online]. W3, publikované v 8/1996 [cit. 25.3.2018]. Dostupné z : www.w3.org/People/Berners-Lee/1996/ppf.html
- LEINER, Barry M. *Brief History of the Internet* [online]. Internet Society, publikované 1997 [cit. 5.11.2017]. Dostupné z: <https://www.internetsociety.org/internet/history-internet/brief-history-internet/>
- LICKLIDER, J.C.R. *The Intergalactic Computer Network: Topics for Discussion at the Forthcoming Meeting* [online]. Publikované 23. 4. 1963 [cit. 5.11.2017]. Dostupné z: <http://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network>
- OECD. *The Economic and Social Role of Internet Intermediaries* [online]. Publikované 4/2017 [cit. 24.3.2018]. Dostupné z: www.oecd.org/internet/ieconomy/44949023.pdf
- Oxford Living Dictionaries. *Definition of Internet in English*. [cit. 29.3.2018]. Dostupné z: en.oxforddictionaries.com/definition/internet
- PANGARO, Paul. *Cybernetics - a definition* [online]. Pangaro, 1990. [cit. 4.4.2018]. Dostupné z: pangaro.com/definition-cybernetics.html
- PELKEY, James. *Entrepreneurial Capitalism and Innovation: A History of Computer Communications 1968-1988* [online]. Chapter 2 Intergalactic Vision to Arpanet, publikované 2007 [cit. 30.3.2018]. Dostupné z: www.historyofcomputercommunications.info/Book/2/2.1-IntergalacticNetwork_1962-1964.html
- POLČÁK, Radim. *Informační teorie práva* [online]. Masarykova univerzita. Učebné materiály predmetu Kritická právní teorie, 2008. s.7 a násl. [cit. 5.4.2018]. Dostupné z: is.muni.cz/el/1422/jaro2008/MVV012468K/um/5626625/polcak-informacni_teorie_prava.pdf
- SAVIN Andrej. *EU Internet Law*. Vyd. 2. Elgar European Law Series, publikované: 28.4.2017 [cit. 25.3.2018]. Dostupné z: www.elgaronline.com/view/9781784717957/10_chapter1.xhtml?
- Swiss Institute of Comparative Law (SICL). *Comparative Study on blocking, filtering and take-down of illegal internet content* [online]. Publikované 20.12.2015, Lausanne [cit. 11.3.2018]. Dostupné z: <https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html>
- Swiss Internet Industry Association. *Hosting Code of Conduct. Notice and take down* [online]. swisscom, publikované 1.2.2013 [cit. 25.3.2018]. Dostupné napr. z: www.swisscom.ch/content/dam/swisscom/en/biz/sme/it-hosting/pdf/wh_verhaltenskodex-simsa_en.pdf
- VONDŘICH, Lukáš. *Mezinárodně-právní aspekty deliktů odpovědnosti na internetu* [online]. Disertační práce. Univerzita Karlova v Praze, Právnická fakulta. Vedúci práce Monika Pauknerová. 2016, s. 54 [cit. 23.3.2018]. Dostupné z: <https://is.cuni.cz/webapps/zzp/detail/146874/>
- VYMĚTAL Petr. *Černé listiny* [online]. Pracovní text pre Ministerstvo vnitra ČR. [cit. 25.3.2018]. Dostupné z: www.mvcr.cz/soubor/studie-vymetal-blacklisting-pdf.aspx
- World Wide Web Foundation. *History of the Web* [online]. [cit. 10.11.2017] Dostupné z: webfoundation.org/about/vision/history-of-the-web/

WU Tim. *A proposal for Network Neutrality*[online]. Publikované 6/2002 [cit. 25.3.2018]. Dostupné z: www.timwu.org/OriginalNNProposal.pdf

3. Zoznam použitých právnych predpisov a stanovísk

Dohovor o ochrane ľudských práv a základných slobôd v znení ustanovení Protokolu č. 14 (CETS No. 194)

Odporúčanie Výboru ministrov Rady Európy CM/Rec(2007)7 pre ministrov členských štátov z 20. júna 2007 o dobrej správe

Odporúčanie Výboru ministrov Rady Európy. CM/Rec(2001)9 of the Committee of Ministers to member states on alternatives to litigation between administrative authorities and private parties

Charta základných práv Európskej Únie (2010/C 83/02)

Nariadenie Európskeho Parlamentu a Rady (EÚ) 2015/2120 z 25. novembra 2015, ktorým sa ustanovujú opatrenia týkajúce sa prístupu k otvorenému internetu a ktorým sa mení smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb a nariadenie (EÚ) č. 531/2012 o roamingu vo verejných mobilných komunikačných sieťach v rámci Únie.

Smernica Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode), smernica o e-obchode

Smernica Európskeho parlamentu a Rady (EÚ) 2015/1535 z 9. septembra 2015, ktorou sa stanovuje postup pri poskytovaní informácií v oblasti technických predpisov a pravidiel vzťahujúcich sa na služby informačnej spoločnosti

Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovania osobných údajov a o ochrane súkromia v sektore elektronických komunikácií

Smernica Európskeho Parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV

Smernica Európskeho Parlamentu a Rady 98/34/ES z 22. júna 1998 ustanovujúca postup pre poskytovanie informácií v oblasti technických noriem a predpisov

Smernica Európskeho Parlamentu a Rady 98/48/ES z 20. júla 1998, novelizujúca smernicu 98/34/ES ustanovujúca postup pre poskytovanie informácií v oblasti technických noriem a predpisov

Odporúčenie Komisie 2014/478/EU zo 14. júla 2014 o zásadách ochrany spotrebiteľov a hráčov využívajúcich služby online hazardných hier a o predchádzaní hraniu online hazardných hier v prípade maloletých osôb.

Report from the Commission to the European Parliament assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography pod COM(2016) 872 final

Body of European Regulators of Electronic Communications. *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules* pod BoR(16)127

Digital Millennium Copyright Act (§ 512 17 USCA)

Ústavný zákon č. 2/1993 Sb., Listina základních práv a svobod

zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů

zákon č. 127/2005 Sb., o elektronických komunikacích

zákon č. 500/2004 Sb., správní řád

zákon č. 150/2002 Sb., soudní správní řád

zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich

zákon č. 101/2000 Sb., o ochraně osobních údajů

zákon č. 40/2009 Sb., trestní zákoník

zákon č. 140/1961 Sb., trestní zákon

zákon č. 40/1964 Sb., občanský zákoník

zákon č. 121/2000 Sb., autorský zákon

Důvodová zpráva k zákonu č. 186/2016 Sb., o hazardních hrách. Sněmovní tisk č. 578/0, Poslanecká sněmovna, 7. volební období

Důvodová zpráva k zákonu č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů Sněmovní tisk č. 579/0, Poslanecká sněmovna, 4. volební období

Ministerstvo Financí. *Metodický pokyn odboru 34 - Státní dozor nad hazardními hrami k plnění povinností ve věci seznamu nepovolených internetových her*) pod č. j.: MF-30513/2016/3402-14

Ministerstvo průmyslu a obchodu. *Digitální Česko v. 2.0, Cesta k digitální ekonomice* [online]. Sekce digitální ekonomiky, publikované 2.4.2013 [cit. 20.3.2018]. www.mpo.cz/assets/cz/e-komunikace-a-posta/Internet/2013/4/Digi_esko_v.2.0.pdf; tisková zpráva: www.mpo.cz/dokument127530.html

Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě č. 104/2013 Sb.m.s.

Swiss Institute of Comparative Law (SICL). *Comparative Study on blocking, filtering and take-down of illegal internet content* [online]. Publikované 20.12.2015, Lausanne [cit. 11.3.2018]. Dostupné z: <https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html>

4. Zoznam použitej judikatúry

Nález Ústavního soudu ze dne 14. února 2017 sp. zn. Pl. ÚS 28/16 ve věci návrhu na zrušení některých ustanovení zákona č. 186/2016 Sb., o hazardních hrách, vyhlášený v Sbírce Zákonů pod Předpis (Nález) č. 95/2017 Sb., částka 37 s účinností od 31.3.2017

Rozhodnutí Nejvyššího soudu České republiky pod sp.zn. 23 Cdo 2623/2011 z dne 31.7.2013

Rozsudok Súdneho dvoru EU z dne 11. septembra 2014, Papasavvas, C-291/13, ECLI:EU:C:2014:2209

Rozsudok Súdneho dvoru EU z dňa 16. februára 2012, SABAM proti Netlog NV, C-360/10, ECLI:EU:C:2012:85

Rozsudok Súdneho dvoru EU z dňa 27. marca 2014, UPC Teleabel Wien GmbH proti Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbh, C-314/12, ECLI:EU:C:2014:19

5. Zoznam podporných internetových a iných zdrojov

Osobná konzultácia s JUDr. Jaromír Hořák , Ph.D. z dňa 22. marca 2018

Blog.CZ.NIC. *STOPonline.cz v detailech* [online]. Publikované 29.11.2017 [cit.17.3.2018]. Dostupné z: <https://blog.nic.cz/2017/11/29/stoponline-cz-v-detailech/>

Body of European Regulators of Electronic Communications. *What is covered and protected by the regulation* [online]. [cit. 13.3.2018]. Dostupné z: bereg.europa.eu/eng/netneutrality/regulation/

COHEN-SHEFFER Natalie. *What is VoIP?* [online]. Viber Blog, publikované 13.11.2017 [cit. 13.3.2018]. Dostupné z: www.viber.com/blog/2017-11-13/what-is-voip/

CZ.NIC. *Vyjádření nesouhlasu k blokování Internetu v rámci zákona o hazardních hrách* [online]. [cit. 20.3.2018]. Dostupné z: www.nic.cz/files/nic/doc/Dopis_blokovani_Internetu-poslanci.pdf

Čo je FCC. Dostupné z: <https://www.fcc.gov/about-fcc/what-we-do>

ČTK. *EU si došlápně na sexuálnimu zneužívání a vykořisťování dětí* [online]. tyden.cz, publikované 14.12.2017 [cit. 17.3.2018]. Dostupné z: www.tyden.cz/rubriky/zahranici/evropa/eu-si-doslapne-na-sexualnimu-zneužívání-a-vykořisťování-dětí_458989.html?showTab=diskutovane

ČTK. *Výsledky voleb: Triumf ANO, fiasko ČSSD, slaví SPD i Piráti* [online]. ceskenoviny.cz, publikované 22.10.2017 [cit. 19.3.2018]. Dostupné z: www.ceskenoviny.cz/zpravy/vysledky-voleb-triumf-ano-fiasko-cssd-slavi-spd-i-pirati-on-line/1540980

ČTÚ. *Mezinárodní roaming a síťová neutralita v roce 2017* [online]. itPoint, publikované 28.12.2015 [cit. 10.3.2017]. Dostupné z: <http://www.itpoint.cz/ctu/clanky/?i=mezinarodni-roaming-sitova-neutralita-2017-10664>

DLA Piper. *EUROPE: New Telecom Package Promoting Net Neutrality Principle Adopted on October 27th, 2015*. Technology Legal Edge, publikované 2.12.2015 [cit. 11.3.2018]. Dostupné z: www.technologyslegaleedge.com/2015/12/europe-new-telecom-package-promoting-net-neutrality-principle-adopted-on-october-27th-2015/

EUROISPA. *Internet blocking: frequently asked questions* [online]. Europe internet services providers association, [cit. 25.3.2018]. Dostupné z: www.euroispa.org/internet-blocking-frequently-asked-questions/

FRENKEL Alex. *Online Censorship: A Global Map & Ranking of Every Country's Internet Restrictions* [online]. vpnmentor, [cit. 15.3.2018]. Dostupné z: <https://www.vpnmentor.com/blog/online-censorship-country-rank/>

GRASSL Gunther. *New EU-Wide Safeguards for Open Internet – EU Regulation 2015/2120* [online]. Schoenherr. Publikované 17.1.2017 [cit. 10.3.2018]. Dostupné z: www.lexology.com/library/detail.aspx?g=5e4ee4fc-f15b-4369-865e-5fc35a8e9af2

CHLUBNÁ Tereza. *Zákon o hazardu prošel sněmovnou. Opozici vadí údajná cenzura internetu* [online]. iRozhlas, publikované 13.4.2016 [cit. 19.3.2018]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/zakon-o-hazardu-prosel-snemovnou-opozici-vadi-udajna-cenzura-internetu_201604131525_dbnardy

Internet Watch Foundation. Dostupné z: <https://www.iwf.org.uk/>

Internet World Stats – Usage and Population Statistics [online]. Dostupné z: www.internetlivestats.com/internet-users/czech-republic/ ku [cit. 1.10.2017], čo odpovedá 88,4% obyvateľstva.

LEVY, Steven. *Hackers at 30: „Hackers “ and „Information wants to be free“*. wired, publikované 21.11.14 [cit. 7.4.2018]. Dostupné z: www.wired.com/story/hackers-at-30-hackers-and-information-wants-to-be-free/

MACICH Jiří. *Telefónica potvrdila filtrování stránek* [online]. Lupa.cz. Publikované 14.8.2009 [cit. 17.3.2018]. Dostupné z: <https://www.lupa.cz/clanky/telefonica-o2-potvrdila-filtrovani-stranek/>

MCDOWEL Robert. Institute for Policy Innovation (IPI) z diskusie o Internetovej regulácii z dňa 12.11.2009. [cit. 14.2.2017]. Dostupné z: https://apps.fcc.gov/edocs_public/attachmatch/DOC-294631A1.pdf

MITCHELL, Bradley. *Understanding Transmission Control Protocol/Internet Protocol (TCP/IP)* [online]. lifewire, publikované: 10. 06. 2017 [cit. 9.11.2017]. Dostupné z: www.lifewire.com/transmission-control-protocol-and-internet-protocol-816255

MURÁNYI, Béla. k informačnej spoločnosti - *információs tarsdálom*. [cit. 24.3.2018]. Dostupné z: <http://comm-media.com/hu/abc/informacios-tarsadalom>

OPAM Kwame. Major telecoms promise 5G networks if EU cripples net neutrality [online]. *TheVerge*, *ArsTechnica*, publikované 12.7.2016 [cit. 25.3.2018]. Dostupné z: www.theverge.com/2016/7/10/12139700/telecom-companies-5g-service-european-union-net-neutrality

Oxford Living Dictionaries. *Definition of Internet in English*. [cit. 29.3.2018]. Dostupné z: en.oxforddictionaries.com/definition/internet

PETERKA, Jiří. *Historie českého internetu: slavíme 10. výročí liberalizace* [online]. eArchiv, publikované: 1.7.2005 [cit. 12.11.2017]. Dostupné z: www.earchiv.cz/b05/b0700002.php3

PRŮŠA Jiří. *Blokování hazardních webů nemá v České republice i Evropě oporu ani obdobu* [online]. CZ.NIC, publikované 29.3.2016 [cit. 20.3.2018]. Dostupné z: blog.nic.cz/2016/03/29/blokovani-hazardnich-webu-nema-v-ceske-republice-i-evrope-oporu-ani-obdobu/

SANDLE, Tim. *UN thinks internet access is a human right* [online]. Digital journal, publikované 22.7.2016 [cit. 28.3.2018]. Dostupné z: <http://www.businessinsider.com/un-says-internet-access-is-a-human-right-2016-7>

SAVICKÝ Jan, *Internet se bude psát s malým i* [online]. Denníku Neviditelný pes v týdni od 22 . septembra do 29. septembra 1997 [cit. 27.3.2018]. Dostupné z webového archívu: web.archive.org/web/20020903231020/http://pes.eunet.cz:80/97/39/0039ar08.htm

Seriál „Jak na Internet“. *Diel 4.5 Historie Internetu* [online]. Publikované v r. 2012-2014 [cit. 9.11.2017]. Dostupné z: www.jaknainternet.cz/page/1205/historie-internetu/

SCHWARTZ John, *The Nation: Case-Sensitive Crusader; Who Owns the Internet? You and i Do* [online]. The New York Times, publikované 29.12.2002 [cit. 27.3.2018]. Dostupné z: www.nytimes.com/2002/12/29/weekinreview/the-nation-case-sensitive-crusader-who-owns-the-internet-you-and-i-do.html

TAANNERU Manav. *Legislation can't keep pace with technology* [online]. CNN, publikované 18.10.2005 [cit. 25.3.2018]. Dostupné z: edition.cnn.com/2005/TECH/10/17/wireless.legislation/index.html

Volné sdružení za psání slova internet s malým písmenem i, aneb Internet versus internet [cit. 27.3.2018]. Dostupné z: <http://web.archive.org/web/20030704002338/www.webhouse.cz/versus/ii/>

VOLLMER, Timothy. *EFF: Fighting for your digital rights for 25 years* [online]. Creative Commons, publikované 10.7.2015 [cit. 7.4.2018]. Dostupné z: creativecommons.org/2015/07/10/eff-fighting-for-your-digital-rights-for-25-years/

ZEMAN Mirek, *Internet vs. internet* [online]. Lupa.cz, publikované 30.8.2004 [cit. 27.3.2018]. Dostupné z: www.lupa.cz/clanky/internet-vs-internet/

slovník-cizích-slov.abz.cz

www.eff.org/about/history

www.internetbezczenzury.cz/

www.jakobejitblokaci.cz/

www.journalistsresource.org/studies/society/internet/net-neutrality-debate-underlying-dynamics-research-perspectives

www.skype.com

www.stoponline.cz/stoponline/

www.youtube.com

Regulace internetu

Abstrakt

Internet je dnes jedným z najrýchlejšie sa vyvíjajúcich technologických nástrojov, ktoré máme k dispozícii. To, čo začalo využitím na výskumné a akademické účely pred štyrmi desaťročiami, sa vyvinulo do virtuálnej komunity, ktorá bola formovaná miliónmi užívateľov. To, čo začalo ako samoregulovaná platforma, vyvoláva vážnu potrebu podrobného prieskumu, pretože stále viac a viac zisťujeme, že súčasný regulačný rámec má masívne medzery a porušovanie ľudských práv je dennou súčasťou rôznych internetových platforiem. Zdá sa, že je len otázkou času, kým dôjde k vážnemu porušeniu ľudských práv alebo dátovej katastrofe. Regulácia vytvorená v dôsledku snahy o zotavenie sa z katastrofy by bola v budúcnosti neprimerane prísna a kontrolujúca, čo by malo za následok stratu mnohých slobôd, ktoré internet poskytol svetu. Vo svetle tejto skutočnosti hľadá táto práca odpovede na tému regulácie internetu. Internet sa rozrástol a vyvíjal exponenciálne a je načase, aby regulácia tohto priestoru dosiahla rovnaký vývoj a bola schopná účinne riadiť a regulovať túto rozsiahlu a viacdimenzionálnu platformu.

Cieľom tejto diplomovej práce bolo teda porozumieť dynamickému vzťahu regulácie a internetu. K preskúmaniu tohoto vzťahu sme analyzovali koncept kyberpriestoru a samostatnosti právneho odvetvia, ktoré sa ním zaoberá. Do úvahy sme vzali východiska metód jeho efektívnej regulácie, a to analýzou špecifik tradičnej regulácie a samoregulácie. V teoretickej časti tejto práce sme vyšli z poznatkov kybernetiky k porozumeniu práva ako informačného systému a metaregulačnej metódy. To sme uplatnili na prostredie kyberpriestoru ako novo vznikajúceho spoločenského systému. Skúmali sme, ktoré entity sú spôsobilé priamo a nepriamo kyberpriestor regulovať na základe zapracovania úvah o regulatívnych modalitách. Naším dosiahnutým poznáním bolo poukázať na ich vzájomný symbiotický vzťah, ktorým dosahujú účel legitímnej a efektívnej organizácie kyberpriestoru. Základom tejto analýzy sa stala teleologická výkladová metóda a právny pragmatizmus. Praktická časť je rozdelená do troch celkov. Prvý celok preskúmava vznik právneho vzťahu zodpovednosti za vlastný a cudzí obsah poskytovateľov služieb informačnej spoločnosti v českom práve. Výklad zodpovednosti nadväzuje na predostretú úvahu o koncepte

gatekeeperov internetu. Predpokladom druhého celku bolo poukázať na obsah v zmysle zásadnej nediskriminácie druhu prenášanej informácie v sieti elektronických komunikácií. Táto znalosť je základom nediskriminačného európskeho prístupu k otvorenému internetu. Detailne popisujeme výsek práv a povinností užívateľov a poskytovateľov služieb pripojenia k internetu, ktoré zakotvujú európsky princíp tzv. sieťovej neutrality. Tretí celok sa vo svetle sieťovej neutrality venuje vybraným problémom blokovania prístupu k určitému obsahu, ktoré sú popísané na dvoch národných modeloch regulačného rámca. Názorne poukážeme na Českú republiku ako príklad modelového štátu s nedostatočným rámcom, na ktorej sme názorne poukázali na špecifické možnosti zamedzenia prístupu k detskej pornografii a detailnou analýzou preskúmali aktuálnu problematiku blokácie nepovolených internetových hazardných hier. Záver práce sa vracia k premietnutiu početných právne technických konceptov, ktorými sa práca zaoberá do metafory progresívneho vývoja civilizácie. Ďalej vyzbrojený poznatkami práce navrhuje ako aktuálne východisko regulačného rámca internetu efektívne nastavený systém metaregulácie.

Klíčová slova: regulácia internetu, kyberpriestor, zodpovednosť, sieťová neutralita

Regulation of Internet

Abstract

The internet is today one of the most rapidly evolving technological tools at our disposal. What started out being used for research and academic purposes over four decades ago, has evolved into a behemoth virtual community that has been shaped by millions of role-players and users. What started out as a self-regulated platform is coming under serious scrutiny as more and more we are finding that the current regulatory framework has massive gaping holes and human rights breaches are happening by the thousands, on a daily basis, across various internet platforms. It seems it is only a matter of time before a serious human rights or data catastrophe is on our hands. Regulation created under the stress of trying to recover from a catastrophe would be strict and have excessively tight controls and result in the loss of many freedoms which the internet has afforded the world. It is in light of this that the topic of the regulation of the internet is explored through this thesis. The internet has grown and evolved exponentially, and it is time that regulation of this space catches up to this evolution and is able to effectively govern and regulate this vast and multidimensional layer.

The aim of this diploma thesis was to understand the dynamic relationship between regulation and the Internet. To explore the relationship, we have analysed the concept of cyberspace and the distinct area of law that it concerns. We took into consideration the primary methods of the effective regulation by analysing the specifics of traditional regulation and self-regulation. In the theoretical portion of this thesis, we have utilized the knowledge of cybernetics, to understand law as an information system and method of meta-regulation. We applied this to the environment of cyberspace: a newly rising social system. We have examined which entities are capable of direct and indirect regulation of cyberspace and deliberated these various modalities of regulation. In conclusion we have determined that a symbiotic relationship between these modalities achieve the purpose of effective and legitimate organization of Cyberspace. The basis for this analysis was the teleological interpretational method and legal pragmatism. The practical portion of the thesis is divided into three sections. The first section explores the establishment of liability of internet service

providers for their own and user-generated content in Czech law. This ISP liability takes into consideration the context of the internet gatekeeper theory. The precondition of the second section was to differentiate content in terms of fundamental non-discrimination of the information type transmitted in the electronic communications network. This knowledge is the basis of a non-discriminatory European approach to open Internet. The rights and obligations of ISPs and users are described in more detail, as a principle for anchoring the concept of network neutrality. The third section, in lieu of network neutrality, addresses selected problems of blocking access to certain content, which are described on two national models of the regulatory framework. Czech Republic is elaborated on as a model state with an insufficient regulatory framework, where we pointed out the specific possibilities of prevention of access to child pornography and provide detailed analysis of the current issue of blocking illegal Internet gambling. The conclusion of the thesis reflects back to the many legal and technical concepts outlined in this thesis and are portrayed in a metaphorical form as the progressive rise of a civilization. Armed with the knowledge we have gathered throughout this thesis, a suggested recourse for the contemporary regulatory framework of the internet was derived to be a meta-regulation system that could provide a suitable internet regulatory framework for the future.

Keywords: regulation of internet, cyberspace, liability, net neutrality